SECURING DISTRIBUTED ENERGY RESOURCE INTEGRATION

BY

MEGAN JORDAN CULLER

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois Urbana-Champaign, 2021

Urbana, Illinois

Advisers:

Professor Peter Sauer
Associate Professor Kirill Levchenko

ABSTRACT

The penetration of distributed energy resources (DER) is growing at much higher rates than predicted 20 years ago. Far from being used only in residential settings, DER are now installed on distribution and transmission circuits. In this position, they do not have the same properties as traditional generators and are more flexible in many cases. The growing penetration and range of uses for DER motivate the need to reliably and safely integrate them into the grid. Operators must be able to rely on them not only for normal operation, but also during abnormal conditions like black starts or adverse cyber scenarios. To that end, we study the communications, device interfaces, and potential consequences of DER operation under abnormal and adversarial conditions. The weaknesses of communications networks are studied based on the industrial protocols used, and the benefits of security features are examined. The device interfaces are found to be vulnerable to attack based on the requirements in the IEEE-1547 standard for DER interconnection and interoperability, which is expected to be adopted in the next ten years. In addition to exploring the requirements of the standard, we show that these vulnerabilities and others do exist and can be used maliciously in a modern storage system DER. Consequences of these vulnerabilities range from exacerbated grid instability, to simultaneous loss of large portions of DER penetration, to physical damage to inverters or DER themselves and other sensitive equipment. We tie these outcomes to specific attacker actions in an effort to give operators a better threat intelligence view that allows them to prioritize mitigations. Finally, we discuss mitigations that could prevent many of the adversarial scenarios described. Some solutions can be added to existing infrastructure, while others may require longer term planning for grid modernization with consideration for security.

To my parents, for their love and support.

ACKNOWLEDGMENTS

Thank you first to my advisors and project managers. I have learned so much from you all. Prof. Sauer, thank you for your stories and encouragement; it means so much to have you advocate for me. Prof. Levchenko, thank you for pushing me to deepen my cybersecurity knowledge. I will use it often in my work, and because of you, I am an amateur expert in aircraft landing procedures. To Al Valdes, thank you for the opportunity to be involved in your projects. They started me on the path of DER integration and will serve me well in the future. To Ginger Wright, thank you for advocating for me in so many ways and for always finding me a place on a project that utilizes my dual passions for power and cybersecurity. I'm still deciding what kind of unicorn I want to be, but it's looking like DER will be part of my core areas of expertise.

To my INL and PNNL colleagues: Thank you to Hannah Burroughs and Emma Steward for your extensive mentorship on the battery project, and of course, for making that project happen. Thank you to Kurt Myers, Porter Hill, and William Parker for your instruction and support in the lab.

Part of the research for this thesis was performed under my role as a Graduate Fellow for Idaho National Laboratory. I am grateful to the program managers and the research staff and for the opportunity to conduct part of my thesis research with INL.

Thank you to my UIUC colleagues - to Prerak Chapagain for taking on this project with me, to Richard Macwan for getting us started, and to Ken Keefe for showing me a new way to view attack graphs.

Thank you to my roommates, Mia, Izzi, and Kyle. You have been my cheerleaders and supporters.

Thank you to Steven. I don't know where I'd be without you and I'm so grateful for your love.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AEPS	Area Electric Power System
APT	Advanced Persistent Threat
CHP	Combined Heat and Power
DER	Distributed Energy Resources
DPI	Deep Packet Inspection
EMS	Energy Management System
ESS	Energy Storage System
EV	Electric Vehicle
HIL	Hardware-in-the-Loop
ICS	Industrial Control Systems
ISO	Independent System Operator
Li-ion	Lithium Ion
MitM	Man-in-the-Middle
PCC	Point of Common Coupling
RTO	Regional Transmission Operator
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SEI	Solid Electrolyte Interphase
SOC	State-of-Charge
VAR	Volt-Amp Reactive
VPN	Virtual Private Network

CHAPTER 1

INTRODUCTION

The United States is experiencing an energy revolution. Due to aging infrastructure, policy changes driven by climate change, shifting economics for new technologies, and a recognized need for long-term sustainability, there is a push towards using clean or carbon-neutral energy sources. On top of that, growing electrification and rising load continue to put a strain on existing transmission and distribution infrastructure. While the energy landscape of the future will require changes and technological advances across the industry, and may take one of many forms, it is clear that distributed energy resources (DER), including solar, wind, and storage, will play a major role.

The energy industry is facing another type of revolutionary change on top of the changes in power production, distribution, and consumption. As new technologies are introduced to make grids smarter, more efficient, and more sustainable, increased control, monitoring, and communication across the power grid is required. However, each new meter, controller, and electronic safety device is a potential target for a cyber adversary. Historically, cybersecurity was not a concern for power systems since they were largely airgapped from any publicly accessible networks. That is no longer the case, and even if appropriate protections are put in place to isolate industrial networks from commercial networks, a motivated and well-resourced adversary may find ways to access sensitive networks or devices that provide critical services.

While electric energy infrastructure may not be the first high-value target people think about for cyberattacks, there has been a rise in cyberattacks targeting industrial control systems (ICS) and a corresponding rise in attacks targeting electric energy systems over the last several years. Dragos Inc. reported in 2020 that threats to ICS are appearing at a rate three times that at which they are going dormant [1]. The energy sector is a high-value target for cyber adversaries because of the immediate and wide-reaching consequences

that a successful attack could have. Large-scale blackouts have consequences not just for our domestic lives, but also for vital health and financial systems [2, 3]. The importance of protecting the power grid has also been identified at a federal policy level. There are 16 critical infrastructure sectors, of which energy is one. Presidential Policy Directive 21, which establishes national policy on critical infrastructure security and resilience, identifies the energy sector as uniquely significant since it provides an "enabling function" across all critical infrastructure sectors [4].

There are a few of attacks on the energy sector worth noting. In December 2015, Russian hackers executed an attack on a Ukrainian distribution company, disconnecting seven substations after infiltrating the supervisory control and data acquisition (SCADA) network and causing blackouts for over 200,000 customers [5]. The outages lasted only a few hours because operators were able to restore a limited capability manual backup mode, but they were noteworthy as the first publicly acknowledged cyberattacks to result in power outages. Attacks occurred again 2016, this time with more advanced, targeted malware, shutting off approximately 20% of Kiev's power [6, 7].

Shortly following these attacks was another that raised concern in the industry, the Triton (or Trisis) malware. This malware was targeted to interfere with the function of Triconex controllers, which are mostly used in safety instrumented systems [8]. This malware was particularly noteworthy because it targeted safety systems, making it clear that the intended outcome was physical breaches of safety. While the particular device targeted is mostly used in the oil and gas sector, similar devices are used widely across the electric energy industry. Accenture and Dragos have not named an attacker for this case, but propose that the advanced capabilities used suggest a nation-state attacker [9, 10]. Over a year after the attack, FireEye Intelligence released evidence that the source of the attack was a Russian government-owned technical research institution.

While operation focused attacks may continue to be the most impactful threat, ransomware attacks are rising in frequency and beginning to target industrial sectors. Traditionally, ransomware targets enterprise systems, but attackers have learned that cyber-physical processes are good targets too. Particularly in the electric energy industry, there is a need for constant availability of systems. If ransomware can shut down resources critical for

operation, companies may be more likely to pay the ransom immediately rather than try to remove the ransomware on their own. The rise of ransomware targeting ICS has been noted by multiple sources [11, 12, 1]. In fact, 33% of ICS companies surveyed by Kaspersky in 2018 indicated that ransomware was one of the top three incidents they were concerned about for their industrial control networks, and 30% indicated that ransomware was a cause of ICS cybersecurity events that they experienced in the previous twelve months [13]. In 2019, a ransomware attack on a natural gas compression facility forced operators to shut down operations for two days [14]. The details of ransomware variant were not made public, but Dragos learned that it was likely the Ryuk ransomware, a variant that was originally tied to the North Korean Lazarus Group, but is now believed to be from a cybercriminal group [15, 16]. This attack started with a spearphishing attack that allowed the adversaries initial access into the system. This is a common starting point for many attacks, and it points to the need for continued employee cybersecurity training. Although the facility could still operate, there was a lack of visibility into real-time and historical data, which made continued operation unsafe. This fact raises a critical consideration: Cyberattacks do not necessarily have to directly impact key processes in order to indirectly shut those processes down.

Finally, and perhaps most noteworthy for this thesis, a cyberattack affecting wind and solar plants in the U.S. occurred in 2019. A vulnerability in the network firewalls was exploited to force the devices to reboot, causing communication outages in five minute periods over a total of twelve hours [17]. This attack did not cause any power outages or stop generation at the DER sites, but it did block visibility into the system and interrupt the ability to make operational changes. Notably, it is not believed that the unknown hackers targeted the energy sector, and they may not have even known what devices they were attacking [18]. This event underscores the vulnerability of the grid to a wide range of attacks, not just nation-state actors, advanced persistent threats (APTs), or financially motivated cybercriminals. If this attack had targeted an entity making frequent active operational decisions, the consequences could have been more severe.

Within the landscape of growing cybersecurity threats to the electric energy industry, the growth of DER presents certain challenges that have not been well addressed. By their nature, DER are distributed, meaning that

individual devices may be separated geographically, and at the least, the devices are not concentrated in a single center the way a traditional power plant is. To manage and monitor these distributed devices requires increased communication, and particularly calls for increased remote communication capabilities. This need is further increased by the fact that many DER may be owned by consumers or third-party aggregators, requiring more coordination on both ends to successfully integrate DER. Remote communication can be especially vulnerable to cyberattacks.

DER can also serve a wider variety of functions than most assets in the power system. Rather than being limited by rotational mechanics, most DER are inverter based, meaning they can ramp power up and down very rapidly, and control active and reactive power separately, which makes them very flexible. However, if these increased capabilities are maliciously used, the benefits they provide to connected grids can quickly become big risk factors. Due to the new and rapid technology development of DER and the risks described above, there is a strong need to evaluate cybersecurity risks and provide proactive prevention, detection, and mitigation solutions.

The rising use of DER presents unique challenges to ensure that power grids are protected from cyberattacks. Cardenas et al. [19] suggest that DER penetration is not yet high enough to pose a significant concern, but if penetration continues to grow, the risks will need to be addressed. It is critical that we address the cybersecurity risks of DER before they are so widely deployed that the cybersecurity risks proposed pose significant danger. Proactive research in DER cybersecurity is the only way we can develop the technology, standards, and policies required to ensure that power and energy infrastructure is well protected.

In this thesis, network and cyber-physical security for DER are analyzed in two ways. In the first part of the thesis, we discuss the communication and interoperability requirements for generic DER and how they can be adversarially manipulated. The focus is on these cyber-physical interactions, as they are unique for DER and require novel cybersecurity solutions. A defense mechanism is proposed to stop these kinds of attacks before they occur by inspecting incoming commands to the DER and evaluating their safety given the current modes active on the device and the current system measurements. In the second part of the thesis, we focus on storage devices as DER. Storage devices by nature can inject and absorb power, which

makes them more interesting to evaluate. Grid stability impacts, battery hardware impacts, and economic impacts of cyberattacks on grid-scale storage are presented. Finally, we present a case study of a real storage device in a field-tested setup. A security analysis is performed on the communications and command interface, and security properties that make the device more robust against attacks are presented.

Although the need for cybersecurity for DER is growing, most research in the field addresses potential attacks based on common network configurations and DER capabilities. This thesis augments previous work by providing a detailed analysis of the vulnerabilities of the IEEE 1547 standard rather than generic functionalities, and by detailing specific impacts of cyberattacks on DER across grid impact, device impact, and economic impact categories. Novel work presented here also shows the feasibility of attacks and the benefits from adding security features to communications protocols. Related work has been done with hardware-in-the-loop simulations, but this work studies cybersecurity on fully deployed hardware systems. While there has been work in the broader areas of attack detection and of deep packet inspection, this work also provides a novel tool to detect attacks specific to DER capabilities.

The rest of the thesis is organized as follows. In Chapter 2, we present background information for power and cybersecurity. In Chapter 3, we present a security analysis of the IEEE 1547 standard. In Chapter 4, a deep packet inspection tool is developed to mitigate the impacts found in the security analysis. In Chapter 5, we focus on storage devices and analyze the consequences of a successful attack for the grid, for the battery hardware, and for utility and consumer economics. Finally, in Chapter 6 we analyze a case study from the perspectives of communication protocol security and physical outcomes of a successful adversarial change to settings. In Chapter 7, conclusions are presented.

CHAPTER 2

BACKGROUND

Reliability and resiliency are major considerations for power systems, but cybersecurity is still a relatively new consideration in the field. Much of the existing work on cyberescurity with power applications focuses on the bulk electric system or on customer-facing endpoints rather than generation sources. DER present a unique challenge in the field because they are generation sources which, in aggregate, can have a significant impact on the grid. However, they can also be owned by consumers, aggregators, or utilities, and thus the security of such devices must be handled differently.

In particular, DER are more likely to require expanded communications interfaces so that they can be operated correctly and send data to all invested parties. The temporal rates, granularity, and content of the communications may change depending on the receiving party, both for operational efficiency and security. This expanded communication interface creates more opportunity for a dedicated adversary to infiltrate the system. Depending on interoperabilty requirements, the DER may transmit data to or receive commands from more than one party, which exposes multiple channels for adversarial exploit. Additionally, the control requirements of DER to handle variable energy sources, grid-support functions, and economic operation means that an adversary may be able to use these controls to execute more impactful attacks.

In this section, we discuss some of the unique challenges around securing DER and how existing research can support this effort.

2.1 Defining DER

There is no standard definition for DER, either in terms of technology or size. However, DER typically refers to smaller, geographically dispersed resources

[20]. DER are typically thought of as distributed solar, wind, or storage applications, although they can also include combined heat and power (CHP) plants or even electric vehicles (EVs). In this work, DER refers to inverter-based DER, and so CHP is out of scope. These generation sources can be contrasted to the historical grid setup, where large centralized generation, typically located further from densely populated areas, produces power. This power is then sent to customers via high voltage transmission lines, and distributed to consumers on lower voltage networks.

The National Association of Regulatory Utility Commissioners defines DER as "a resource sited close to customers that can provide all or some of their immediate electric and power needs and can also be used by the system to either reduce demand (such as energy efficiency) or provide supply to satisfy the energy, capacity, or ancillary service needs of the distribution grid. The resources, if providing electricity or thermal energy, are small in scale, connected to the distribution system, and close to load" [21]. This definition speaks to some of the key characteristics of DER that are discussed from a cybersecurity perspective. Namely, the ability to provide ancillary services to the grid and support local load are key benefits of DER, which, if manipulated by a cyber adversary, can have wide-reaching impact.

The Electric Power Research Institute (EPRI) has a more quantitative definition of DER: "Distributed Energy Resources (DER) are electricity supply sources that fulfill the first criterion, and one of the second, third or fourth criteria:

1. Interconnected to the electric grid, in an approved manner, at or below IEEE medium voltage (69 kV).

2. Generate electricity using any primary fuel source.

3. Store energy and can supply electricity to the grid from that reservoir.

4. Involve load changes undertaken by end-use (retail) customers specifically in response to price or other inducements or arrangements" [22].

DER may be configured in many ways. It may be a single solar panel or wind turbine used for education and research at a university. It may be consumer rooftop solar. It could be an industrial scale combined storage and solar system to offset power consumed at a manufacturing plant or data

center. It could be small wind or solar farms integrated at the distribution level for utilities. These examples are mentioned to demonstrate the range of applications. From an architecture standpoint, the takeaway is that DER may be installed individually, groups of DER may be managed by an aggregator, or they may be directly managed by a utility. Even different types of physically separated DER can be jointly managed as a virtual power plant.

2.2 Grid Support and Ancillary Services

Modern DER can be used to provide many critical services. These can be broken down by services or functionalities that must be specifically built into the DER design, and services that the DER can provide by the nature of distributed generation.

Functionalities that DER are designed to provide include the following, as identified by Sadan and Renz [23]:

- **Volt-VAR support:** Reactive power output is a dynamic response to changes in local voltage. Typically, when voltage is low, reactive power is injected to drive voltage up towards nominal, and when voltage is high, reactive power is absorbed to drive voltage down towards nominal.

- **Frequency-Watt support:** Active power output is a dynamic response to changes in frequency. Typically, when frequency is low, active power is injected, and when frequency is high, active power is absorbed.

- **Voltage ride-through:** The sudden disconnect of generation sources in response to small voltage deviations can cause cascading failures. To prevent this, DER may be required to "ride through" the voltage deviations. This means that they must stay connected during the disturbances for a certain amount of time to try to help the system return to stability. If after a certain time, the unstable conditions still persist, the DER should trip off.

- **Frequency ride-through:** Similar to voltage ride-through, frequency ride-through requires that DER stay connected for a period of time when frequency deviations occur. If the deviation persists after a period

of time, the DER should disconnect from the system, an action known as tripping off.

- **Intelligent Volt-Watt control:** Active power is adjusted based on the current voltage. While this typically has less of an effect than Volt-VAR mode, it can still be a useful tool, especially when there is more control over active power output.

- **Storage system charge and discharge management:** The ramp up and ramp down rates for storage systems can be limited so there are not sudden changes. It may also require that the storage device maintain a certain state-of-charge to protect the battery and equipment.

- **DER protection: island detection and grid-disconnect:** Due to the distributed nature of DER, a fault that disconnects part of the grid may cause DER to energize local parts of the system that should be de-energized after the fault. DER should detect if they have formed an unintentional island and should disconnect.

- **Grid-form on an intentional island:** DER should not energize parts of the system if it is not pre-scheduled, but they may be part of an intentional island or microgrid. They may even be a primary source for this island. In this mode, the output of the DER should be adjusted to maintain voltage and frequency at particular setpoints.

- **Max generation limiting:** In some setups, DER should not export energy to their grid and should not back feed energy. Output may need to be limited (often called curtailing) to meet this requirement.

- **DER load balancing:** DER output may need to dynamically respond to changing load. As load comes online, DER should increase their power output. If loads drop off, DER should decrease their power output.

By the nature of acting as distributed generation sources, DER can provide transmission congestion relief and microgrid or islanding support. They can serve local load, preventing a utility from having to supply as much load.

Cyberattacks can interfere with any of these critical services, and the impacts of such attacks are described in detail in Chapter 5.

2.3 IEEE 1547-2018 Standard

The previous section discussed some generic features and services that DER can provide. This thesis does significant analysis of the IEEE 1547 standard, which sets requirements around many of these functions and the communications required to support these functions. Some background and history is provided here, and the details necessary for the security analysis are explained in Chapter 3.

The IEEE 1547 standard was originally published in 2003. At the time, DER penetration was low, so the standard required DER to trip off (disconnect from the connected system) in response to even minor disturbances, so operators would not have to worry about these emerging technologies when handling disturbances. They did not consider continuous DER operation important to the grid [24]. Since then, DER have grown at much faster rates than expected. Policy makers across the United States and around the world have set aggressive goals for clean energy or carbon-neutral energy production. California is targeting 50% clean renewable energy by 2030, Hawaii is targeting 100% clean energy by 2045, and New York is targeting 70% renewable energy by 2030 [25, 26, 27]. In fact, as of 2020, 30 states have renewable portfolio standards, and of these, 22 specifically set targets for distributed generation or solar [28]. Clean and renewable energy can come from a variety of sources including nuclear, geothermal, or hydro. Bulk solar and bulk wind will also contribute. On top of contributions from all of these sources, DER like distributed wind, distributed solar, and grid-scale storage will undoubtedly play a role in meeting renewable portfolio standards.

With the current and projected growth of DER, the 2003 recommendation for DER to trip immediately is no longer the best recommendation. In systems with high penetration of DER, the simultaneous tripping of the DER would likely make any disturbances worse. The new standard requires that DER provide reactive power support, ride through disturbances, and only trip off after certain thresholds are reached.

2.4 Communication Interfaces

In order to support the grid functions most efficiently, DER connected to distribution systems are required to communicate with the utility. IEEE 1547, California Rule 21, and Hawaii Rule 14H all require that grid-connected DER provide frequency and voltage ride-through function, Volt-VAR support, and some mix of other grid support functions [29, 30, 31]. In order to effectively perform these functions, communications with the utility are required. The utility must instruct the DER how much reactive power support to provide in response to voltage deviations based on the rest of the system configuration. Similarly, the utility must assess the rest of the system to determine how long DER should ride through disturbances. In systems with high DER penetration, the sudden loss of high amounts of generation will be more damaging, so those DER will require longer ride-through settings. Long term and continuously available communication infrastructure is required because these settings may need to change based on dynamic operation of the grid; for example, they may change based on what other generation sources are currently online or what the current load level is. Additionally, communications with an aggregator, if one exists, are mandatory. The owner of the DER may be separate from both the utility and the aggregator, and in this case communications including control, health monitoring, or performance monitoring may also be required. All of these increased capabilities for DER, driven by policy and technology, will require increased communications and communications infrastructure to safely operate power systems [32].

These communications will all have to use network protocols. IEEE 1547 specifically calls out DNP3, SEP2, and Sunspec Modbus as being options for communications with DER, but other protocols are possible [33, 34, 35]. Historically, protocols used in power system networks were designed with latency and performance as key factors, and as a result, the protocols used were largely unsecured [36]. While latency is still a huge concern, security is now being factored into decisions about communications too [37, 38, 39]. It is worth noting that not all communications have the same latency requirements. Safety-critical messages, for example those used for communications-based islanding detection, require very low communications latency. Others, like changing setpoints on a Volt-VAR curve, may not be as time sensitive. However, to ensure all requirements are met, most infrastructure is still

built to satisfy the most constrained latency requirements. Other research discusses network security for DER in detail and provides key recommendations that align with general cybersecurity best practices [40]. In this work, we evaluate with real power and communications hardware what benefits can be provided by using a protocol with more security features (see Chapter 6).

An additional characteristic of DER communications is the need for remote communication. Unlike centralized power plants, the DER under a utility's domain may be geographically separated and difficult to access. Remote access via cellular or wireless links has been touted as a feature of new technologies, but remote connections pose a particular danger from a cybersecurity perspective. If these links are not well secured, it may be simple for an attacker to spoof messages to or from a DER device remotely. Most communications will take place over private channels, whether this is physically private connections, dedicated telephone company circuits, or a virtual private network (VPN). This is not universally the case though. More and more devices require communications over the internet. Suppliers say this gives them the ability to monitor device health and perform preventative maintenance. Many suppliers also have custom applications that customers can log in to to access their device's data. Any traffic sent over the internet should be treated with caution. Research has demonstrated the potential for this attack, with many smart grid components identified via Shodan [41].

2.5 Safe and Secure Grid Operation

The ultimate goal of integrating DER into the grid is to make the grid more resilient and reliable, and to ensure continued safe and secure delivery of electric energy to end-users. These terms can mean different things in different contexts, so we define important terms as they are used in this thesis.

2.5.1 Reliability

According to the North American Electric Reliability Corporation (NERC), reliable operation means "operating the elements of the [Bulk-Power System] within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system

will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements" [42]. It is important to note here that this definition talks about uncontrolled separation, cascading failures, and sudden disturbances. This is not equivalent to keeping power on for all customers at all times.

2.5.2 Resiliency

According to Presidential Policy Directive 21 (PPD21), resiliency means "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents" [4]. Many organizations use similar definitions. Resiliency is often thought of as robustness against "high impact, low probability" events. This differs from reliability, which is considered as robustness against "low impact, high probability" events. This term also speaks more to the goal of keeping power on for all customers as much as possible.

2.5.3 Security

PPD21 defines security as "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters" [4]. The important aspects here are the concepts of risk assessment, prioritizing risk, and mitigating risk. Cybersecurity is not explicitly called out, but this definition of security can easily be applied to cybersecurity.

CHAPTER 3

SECURITY ANALYSIS OF THE IEEE 1547 STANDARD

3.1 Introduction to IEEE 1547 Standard

The IEEE 1547 standard governs the interconnection between DER and the area electric power system (AEPS) and sets interoperabilty standards. It specifies operational requirements around reactive power capabilities, ride-through requirements, and mandatory tripping points. It also defines the communications interface required to support these functions [29]. The latest version, published in 2018, significantly increases the requirements for DER to provide certain supporting services and to ride through certain disturbances. With these increased capabilities, particularly the specific communications requirements set to enable more services, comes increased cybersecurity risks. We analyzed the requirements of the new standard and found that certain combinations of settings, while compliant with the standard, have the potential to create instability on the DER circuit and connected system.[1] The standard was updated specifically to increase stability, so the threat of a cyberattack causing instability is particularly noteworthy.

While the main part of the IEEE 1547 standard talks only about operational and communications requirements, the committee has not ignored cybersecurity. The latest version IEEE 1547.3 standard is not yet published,

[1]The material in this chapter is based upon work supported by the Department of Energy under Award Number DE-OE0000896. Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

but it will address best practices for DER cybersecurity. The revised IEEE 1547.3 standard is expected to address best practices around setting up secure communications channels and securing devices. The work reported below complements these recommendations by considering an adversary who creates combinations of settings that are standard-compliant but potentially destabilizing.

We present five use cases that demonstrate the potential for malicious mode and setpoint combinations, and one for false data injection.

3.2 IEEE 1547 Active and Reactive Power Modes

The IEEE 1547 standard specifies the way in which active and reactive power output will be chosen based on different modes for active and reactive power. Understanding these modes is critical to crafting an attack that takes advantage of the capabilities.

The reactive power modes are:

1. Constant Power Factor Mode: The AEPS sets a ratio of active to reactive power, known as the power factor, that the DER must maintain.

2. Voltage Reactive Power Mode (Volt-VAR): The AEPS can designate a Volt-VAR support curve that changes the amount of reactive power output based on the measured voltage at the point of common coupling (PCC). Typically, this curve specifies that reactive power is injected when voltage is low and absorbed when voltage is high, both operations which will drive local voltage back towards nominal. A typical Volt-VAR curve is shown in Figure 3.1.

3. Active Power-Reactive Power Mode (Watt-VAR): The AEPS can designate a curve that changes the amount of reactive power output based on the current active power output. The default Watt-VAR curve is shown in Figure 3.2.

4. Constant Reactive Power Mode: The AEPS can designate a constant reactive power output (injection or absorption) while the mode is active.

One and only one of the reactive power modes must be enabled at all times; they cannot be enabled simultaneously.

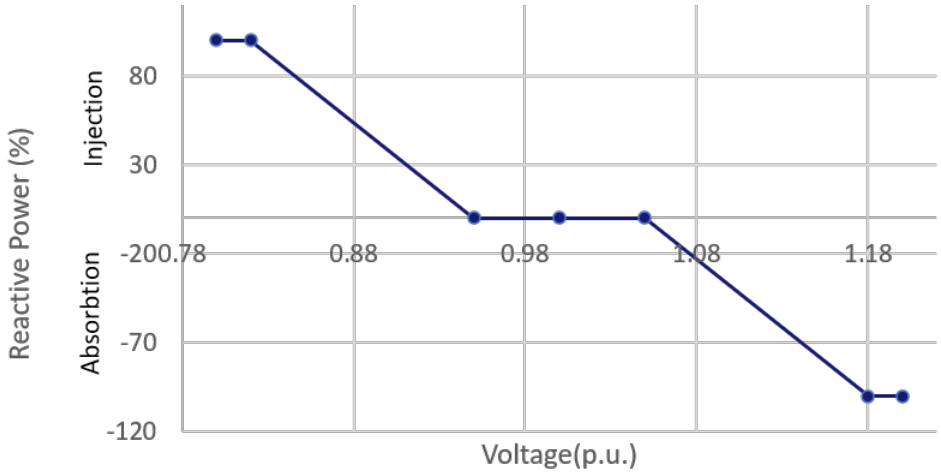


Figure 3.1: Default Volt-VAR curve as specified by IEEE 1547.

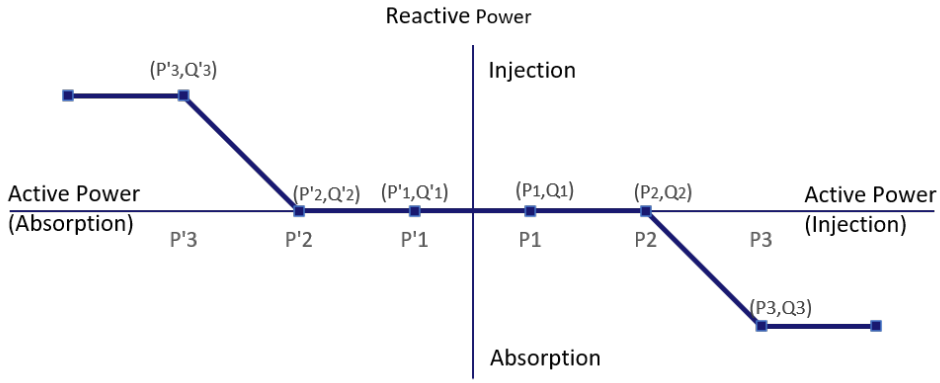


Figure 3.2: Default Watt-VAR curve as specified by IEEE 1547.

There is also a single active power mode called Voltage-Active Power mode (Volt-Watt). If this mode is enabled, the active power output is governed based on the current voltage, and the exact output is determined by a Volt-Watt curve. The default settings for this curve are shown in Figure 3.3. Volt-Watt mode can be enabled or disabled in combination with whichever reactive power mode is active.

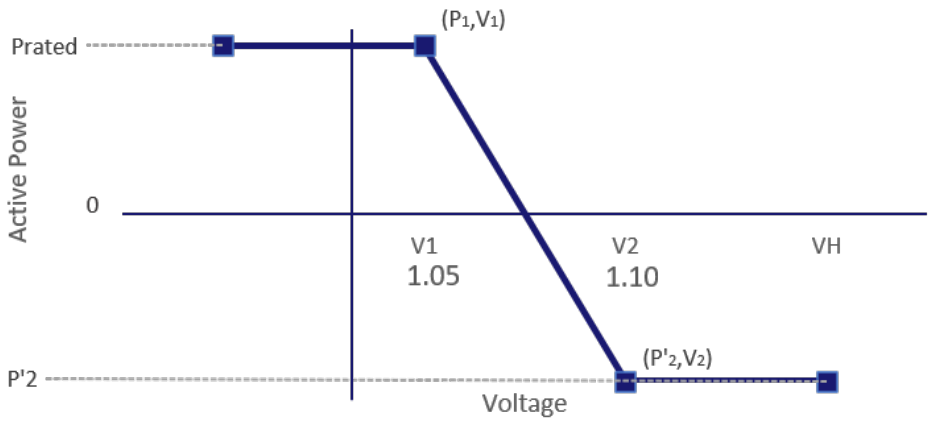


Figure 3.3: Default Volt-Watt curve as specified by IEEE 1547.

3.3 Threat Model

To perform the security analysis, we must first qualify the parameters of the attacks that we consider. In this analysis, we assume that the attacker has the ability to send correctly formatted, valid (via authentication or basic source spoofing) commands to the DER. This could happen via a compromised utility or command center, or the attacker could break protocol security and spoof a valid source.

We assume that the attacker is constrained to valid messages, or that the implementation will reject messages that are not compliant with IEEE 1547. Another way to say this is that we do not consider implementation vulnerabilities of the standard.

The security analysis considers the cyber-physical impacts of different potentially malicious commands that the attacker may send.

3.4 System Model for Use Cases

For the purposes of analyzing the standard and creating simple models to demonstrate the feasibility of these attacks, we use a very simple system model adapted from the author's publication [43], shown in Figure 3.4. This system consists of two DER circuits connected to a larger AEPS with two individual PCCs. Each DER circuit consists of a variable load and an inverter-

controlled energy storage system (ESS) that is capable of generating and absorbing both active and reactive power. The analysis we perform is valid for circuits more complex than our single ESS model, but we make this simplification so that we can assume the DER circuit can inject and absorb both active and reactive power. The single ESS in the model may represent multiple different DER generation sources and local loads. Although the ESS is chosen to allow for a wider range of potential attacks, we keep the security analysis focused on generic DER as much as possible.

The power infrastructure and network infrastructure is shown here. The commands are sent from the Energy Management System (EMS) through the SCADA system to the ESS controller. Each PCC is equipped with a network switch that processes the incoming command from the ESS. The command is forwarded to the ESS controller.

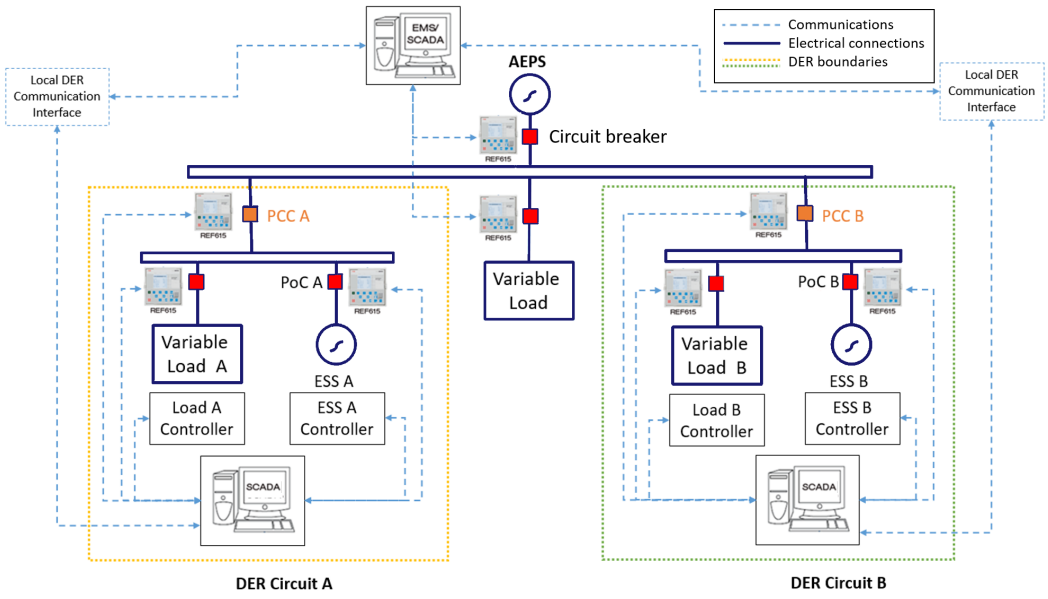


Figure 3.4: Simplified model for IEEE 1547 Analysis, adapted from [43].

For this analysis, we assume that the DER is connected to a medium-voltage AEPS, modeled as a single, limited capacity, synchronous generator and a variable load for the purposes of this model. We also assume that these DER circuits represent a large portion the AEPS capacity, while in practice it may be that many DER in aggregate form a significant portion of the AEPS capacity.

For each DER circuit, a controller such as e-mesh^{TM} SCADA [44] acts as the substation remote terminal unit (RTU) for all the communications on

the DER circuit. It also acts as a gateway that meets the requirements for the DER communication interface in the standard.

The circuit breaker connected to the AEPS is considered to be the island breaker. It is in the open position while either one or both of the PCCs are in a closed position to simulate intentional or unintentional islanding.

We make the assumption that the attacker can access the IEEE 1547 compliant communication interface between the AEPS and the DER, but does not necessarily have visibility into the rest of the system, the details of which are not included in our model.

3.5 Use Cases

The following are results from our security impacts analysis of the IEEE 1547 standard. Each use case describes in detail the commands an attacker would have to send, the system states that make the system most vulnerable, and the cyber-physical impacts of a successful attack.

3.5.1 Use Case 1: Malicious Changes to Volt-VAR Mode

In this scenario, the attacker changes the setpoints of the Volt-VAR support curve. This is a simple attack proposed for DER since the Volt-VAR functionality is one of the most basic functions a DER can have. The attacker modifies the curve in such a way that the DER is highly sensitive to changes in voltage and responds to voltage deviations with destabilizing behavior. This attack can be combined with conservative voltage tripping settings to cause DER to trip rapidly in response to conditions that they would normally have been able to ride through.

We assume that the attacker knows some basic information about the system topology and may use this information to infer what will be the most damaging Volt-VAR curve to set. This is not a strict requirement for the attack to be successful, but it will help make it most effective.

A default Volt-VAR curve was shown in Figure 3.1. However, there are large ranges for the reactive power and voltage setpoints allowed by the IEEE 1547 standard, allowing for operators to pick the best voltage support curves

for their system. The standard even warns that improper selection of these values may cause instability, but the options are still there.

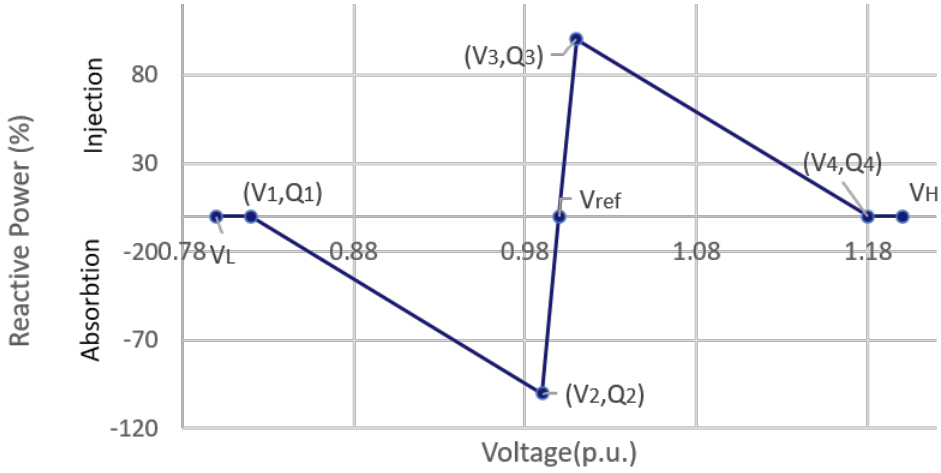


Figure 3.5: Use Case 1: Inverse Volt-VAR curve.

Figure 3.5 shows an example of a malicious curve that is within the allowed bounds of IEEE 1547. In this scenario, a small deviation from nominal voltage would cause rapid injection or absorption of reactive power. Additionally, a drop in voltage will cause reactive power to be absorbed, which will further decrease the voltage. If the attacker also sets the undervoltage tripping requirements to be conservative, for example a clearing time of 2.0 s when the voltage is 0.88 p.u., then once the DER PCC voltage crosses the threshold of 0.88 p.u., a timer starts. At this point, reactive power is still being absorbed, potentially driving the voltage down even lower. After two seconds, the DER must trip, and the AEPS loses this DER as a generation source. The same type of analysis holds for an overvoltage scenario.

There are other possible settings that could create similar destabilizing effects, for example, always injecting maximum reactive power allowed in response to any voltage to drive the voltage up. Conversely, absorbing maximum reactive power allowed in response to any voltage may drive the voltage down.

Potential Mitigations

A sanity check of the setpoints at fixed time intervals could potentially catch any malicious settings. It may also be possible to catch the attack before it happens by using a packet analyzer of network traffic to detect unusual setpoint changes before they reach the DER interface. See Chapter 4 for more details about this mitigation strategy.

3.5.2 Use Case 2: Malicious Changes of Constant VAR Mode

In this scenario, the adversary sets the reactive power mode to Constant Reactive Power and tries to drive voltage up or down in order to reach tripping limits and force a disconnect from the AEPS. Unlike Use Case 1, the attacker actively chooses the precise reactive power output rather than allowing the system to respond dynamically to the voltage. It gives the adversary more precise control over the DER output, but requires more active interaction and monitoring by the adversary. We assume that the adversary has some visibility into real-time measurements. This is not strictly necessary, but will help the attacker choose the most effective attack.

The most obvious choices for the attacker would be maximum rated reactive power injection or maximum rated reactive power absorption. Maximum injection is most likely to drive the voltage up, and maximum absorption is more likely to drive the voltage down. Some systems may require constant reactive power injection near the end of distribution feeders anyway, since voltage tends to droop as it travels over longer distances. Knowledge of system topology and current behavior of the DER will help the adversary choose an output that is most likely to cause instability.

The advantage of this Use Case over Use Case 1 from the adversary's perspective is that the reactive power output is not dependent on the voltage. The adversary may choose 100% reactive power injection, and the system will continue to provide that even as the voltage passes critical points. Also, this mode allows the attacker to choose a desired output regardless of fluctuations in the voltage.

The disadvantage of this attack compared to Use Case 1 from the adversary's perspective is that it may require more active monitoring. In Use Case 1, the adversary can change the Volt-VAR setpoints and leave them. Here,

the attacker must know and choose the setpoint that will most effectively disrupt the system. Another disadvantage is that Use Case 2 may be more likely to be detected than Use Case 1. System operators may be more likely to trust that Volt-VAR support is occurring as expected, and may not initially suspect that this mode is corrupted. However, it would seem more natural to notice that if Constant Reactive Power mode is active and operating at a bad setpoint. This is predicated on the idea that someone is actively monitoring the DER mode, which would depend heavily on how the DER were deployed.

3.5.3 Use Case 3: Malicious Changes to Volt-Watt Mode

In this scenario, the attacker changes the setpoint of the Volt-Watt mode regulating active power output. We assume that the AEPS is operating at low load, and the voltage at the PCC may be trending on the high side of normal bounds. Namely, this means that with Volt-Watt mode enabled, the DER circuit is absorbing maximum rated active power.

The attacker maliciously modifies the points of the Volt-Watt curve (see Figure 3.3) so that that at V_2, the active power is 0, $P_2' = 0$, which is the maximum allowed setpoint for DER that are capable of absorbing power. The DER circuit changes from absorbing maximum rated active power to zero active power output. The AEPS sees this as a drop in load equivalent to the rated active power capacity of the DER circuit. The change may cause the high voltage to rise even higher, potentially forcing tripping conditions.

3.5.4 Use Case 4: Introduction of Contradictory Modes

We assume that the operation point at the beginning of the attack is one where the DER is operating as a generation source, injecting both active and reactive power into the AEPS. To execute the attack, the adversary ensures that Volt-Watt mode is enabled by checking the current settings and sending a command to enable this mode if it is not currently on. This ensures that the active power output is at rated maximum injection if the voltage is at or below nominal levels. Then, the adversary sends a command to change the reactive power mode to Watt-VAR modes. Since we already know active power output

is at maximum injection, reactive power output will be determined by this active power output, which according to the default curve will be maximum rated reactive power absorption. See Figure 3.6 for a visualization of the change in operating points.

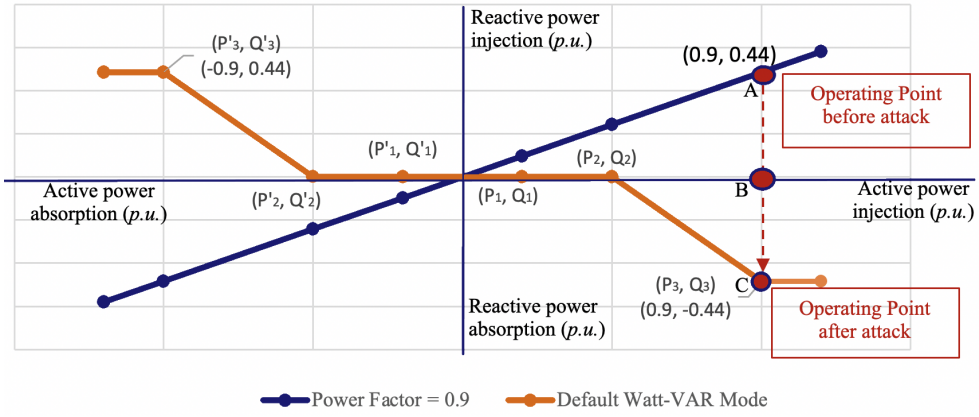


Figure 3.6: Use Case 4: Change in operating point, adapted from [43].

The change from high reactive power injection to high reactive power absorption causes a decrease in local voltage. However, because the Volt-Watt curve specifies continued injection of maximum rated active power as the voltage drops, the reactive power output will also remain at maximum absorption.

The effect of this change in operating point will depend on the penetration of DER into the system. If this attack is carried out against all DER in the system, and collectively they represent a significant proportion of the total generation capacity, then the remainder of the AEPS may not be able to counteract the voltage drop and breakers may trip. However, if the affected DER collectively represent a small portion of the AEPS capacity, then the effect of their misbehavior will be less significant. Extensive work was performed by the author's colleagues on this project to determine the exact penetration of DER on which this attack would have to be carried out in order for the system to collapse [43].

3.5.5 Use Case 5: Permissive Tripping Settings

In this scenario, the attacker selects very permissive tripping requirements so that when grid disturbance events occur, up to and including unintentional

islands forming, the DER does not respond as quickly as it should. This is similar to setting ride-through periods to their maximum limit. The permissive tripping settings that the adversary chooses are those that are farthest away from nominal values and have the longest tripping times. The DER stays connected (rides through) longer than it should.

This is particularly damaging in the case that an unintentional island has formed. When intentional islands form, whether scheduled or unscheduled, the equipment within the island boundaries has all been rated and approved to be part of the island. However, when an unintentional island forms, it may include part of the AEPS that was not approved to be part of an island. It may only expect to transfer unidirectionally, and the unintentional island may cause some devices, like transformers, to be back energized, which causes costly damage and safety hazards.

This attack will be most effective when passive islanding detection schemes are used because these methods rely solely on local measurements, as opposed to active detection or communication-based detection. Active detection uses perturbations that cause voltage or frequency to drift away from nominal until a tripping setpoint is reached [45, 46]. Communication-based detection like Direct Transfer Trip and Phase Comparison rely on coordination and messages sent via the SCADA system from the point where the island was formed [47, 48]. Depending on how the system is configured, there may be separate "islanding detection setpoints" that are separate from the mandatory IEEE 1547 tripping requirements. However, if a simple passive detection scheme is used, it would not make sense to have these be different values.

It is worth noting that failing to quickly detect unintentional islands is not the only consequence of the permissive tripping settings, but it is the most extreme scenario. Other grid disturbance events that do not create unintentional islands could still cause equipment damage under this attack.

It is also worth noting that if the tripping requirements on the DER are already fairly permissive, or if the system is robust to changes in voltage and frequency, then this attack may not have the desired effect. Attack success does rely on an external event happening rather than the adversary triggering an event at a particular time. The effects may still be destabilizing, especially in a system with high DER penetration that all experience the same attack.

3.5.6 Use Case 6: Changing Reported State-of-Charge

One of the communication requirements of the IEEE 1547 standard is that the AEPS can access all of the real-time monitoring information from the DER circuit. In this scenario, the attacker maliciously falsifies some or all of the monitoring information from the DER circuit before it reaches the AEPS. For the scenario discussed here, the DER circuit is assumed to include a storage unit in the form of one or more rechargeable batteries, and the information falsified is the reported state-of-charge.

We make the assumption that the AEPS operator uses the real-time monitoring information to make operational decisions, and thus falsifying this information will have an effect on the decisions made. For this scenario, we assume that the DER circuit is operating in Volt-Watt mode, following the curve in Figure 3.3. If the system is not already in this state, the adversary can send a command to activate this mode.

The SOC of the DER circuit is one of the monitoring information data points available, if applicable to the DER circuit. The attacker maliciously changes the operational SOC data to 100%, when in fact it is at 20%. We note that the standard specifies that the DER circuit shall not be required to reduce active power below the level needed to support local loads, which are assumed to be 20% of the total nameplate rating of the DER circuit. In order to keep the adversarial changes within the scope of valid 1547 operations, the adversary cannot require the DER to lower its active power output below this amount if the DER are being used to support local load. Since in Volt-Watt mode, the DER circuit is required to supply rated active power to the AEPS, the DER circuit will not be able to support its local loads, or it will break its contractual agreement to the AEPS. This can cause local load shedding in the DER circuit along with possible frequency instability at the PCC.

Potential Mitigations

Encrypting communications can make it more difficult for an adversary to execute a false data injection (FDI) attack. If encryption is used, the adversary would have to break the encryption or steal credentials from somewhere they are stored.

On the cyber-physical side, the AEPS operator can infer the operational

state-of-charge (SOC) using frequency and active power measurements at the PCC to independently track the expected SOC and raise alerts if discrepancies are observed.

3.6 Related Work

Work in the last five years has grown around cybersecurity specifically for DER, but there are still few publications on the topic. Sebastian and Hahn discuss DER interconnection standards and smart inverter functions in detail, then discuss the potential attack surface using communication networks and attacking smart inverter functions [49]. They propose metrics to evaluate the impact of attacks. Other research presents network attacks on DER in more detail and provides recommendations that align with standard best practices for cybersecurity are discussed with application to DER [50]. Additional threat assessment work proposes a framework to evaluate the current security position and help stakeholders ensure that they have covered all basic cybersecurity best practices via standards, certifications, and testing against an individual system [51].

CHAPTER 4

MITIGATIONS

In this chapter, a specific mitigation strategy is proposed to prevent cyber-physical attacks on DER by detecting incoming commands that are malicious and blocking them before they ever reach the controller.[1] Since the focus of the thesis is on cyber-physical effects of cyberattacks, this mitigation tool focuses on cyber-physical defenses. There are many existing works that discuss how to detect attacks based solely on the cyber information in packet headers. This chapter instead focuses on application-aware mitigation practices unique to the attacks proposed in Chapter 3.

4.1 Deep Packet Inspection Tool

Many of the attacks described in Chapter 3 involve updating parameters on the DER communications interface which, given the context of the system and the current operating mode, can be labeled as potentially destabilizing. This is not to say that the limits in the IEEE 1547 standard are poorly designed. They are built to be flexible for different systems that use different DER technologies in different applications. Rather, given some information about the current operating state and other system values, the adversary can choose a combination of settings that can destabilize the system.

The mitigation of this kind of command spoofing attack lends itself to deep packet inspection (DPI), a technique by which one can inspect the body of incoming communication packets to the DER controller and determine if their contents are acceptable. This differs from stateful packet inspection, which only looks at the headers of a packet.

[1]The material in this chapter is based upon work supported by the Department of Energy under Award Number DE-OE0000896.

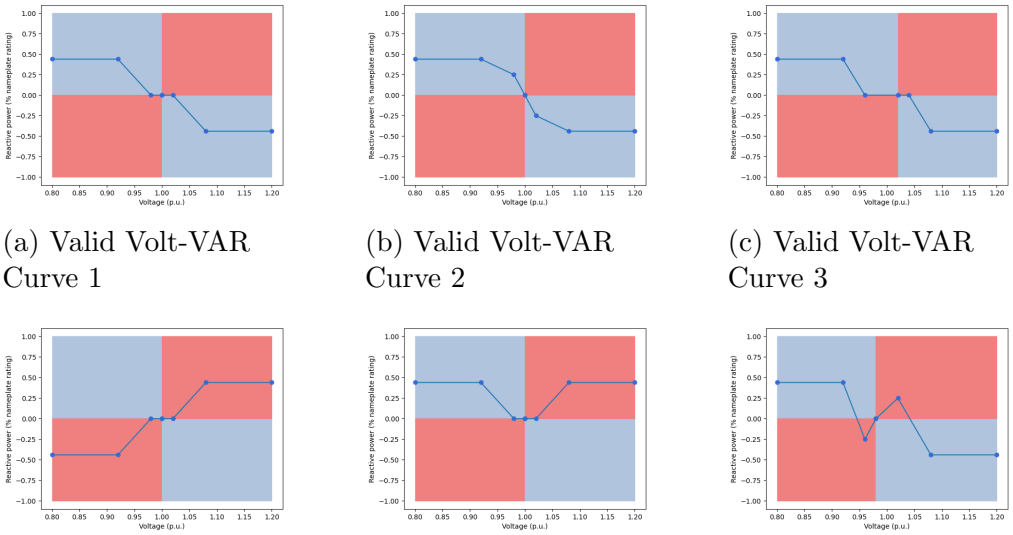
4.2 DPI Tool Development

The purpose of this tool is to demonstrate that it is possible to prevent dangerous commands from ever reaching the DER controller by performing deep packet inspection. Because the decision to forward or drop the incoming command is made solely based on the contents of the packet and current state information, the decision was made to keep the tool protocol-agnostic. IEEE 1547 specifically calls out Sunspec Modbus and DNP3 for communications. The Conformance Test Procedures (IEEE 1547.1) also provide a reference mapping to IEC 61850 [52, 53]. However, since no commercial products are yet IEEE 1547-2018 certified, there are no existing encoders or decoders. By keeping the tool protocol agnostic, we avoid making decisions about implementation that might not hold true for all implementations. More importantly, we make it clear that attacks on the communication protocol are out of scope.

The tool effectively monitors incoming commands, then uses state information and current configuration information from the DER to decide whether the command should be forwarded or dropped. The decision is made based on a series of rules. If the command passes all of the checks, it is forwarded. If it fails some check, it is dropped and an alert is generated for the operator.

The DPI tool takes in commands that change the management information of a DER. It polls a file or server that has the most recent status of the DER and the state information at the PCC, like voltage and frequency. This can be static information, or can be linked to Simulink model running in real time, which publishes the current information or save it to a file. The DPI tool then executes a series of checks against the rules. If the incoming command violates any rule, an error message is displayed to the user interface.

In the current state of development, the packet is not forwarded even if all of the rules are passed. There is work in progress to link the DPI back to the Simulink model to see the effects of accepting or rejecting a packet. Namely, we wish to demonstrate three cases: 1) stable operation when a valid command is accepted and received by the DER, 2) stable operation when an invalid command is rejected, and 3) unstable operation when the DPI tool is turned off and an invalid command is received by the DER.



(a) Valid Volt-VAR Curve 1

(b) Valid Volt-VAR Curve 2

(c) Valid Volt-VAR Curve 3

(d) Invalid Volt-VAR Curve 1

(e) Invalid Volt-VAR Curve 2

(f) Invalid Volt-VAR Curve 3

Figure 4.1: Examples of DPI used to detect valid and invalid Volt-VAR curves.

4.2.1 Volt-VAR Detection

We use the engineering controls adapted from [54] to prevent potentially harmful Volt-VAR curves from being set by an adversary. The determination of the boundaries for allowed and disallowed points is made by the placement of V_{ref} and the zero reactive power line, where V_{ref} is the reference voltage. Points that are below V_{ref} and below zero reactive power suggest absorbing power in low voltage scenarios, which is dangerous and should be rejected. Points that are above V_{ref} and above zero reactive power suggest injecting reactive power in high voltage scenarios, which should also be rejected.

Figure 4.1 shows the results from sending multiple commands with different Volt-VAR setpoints. For visual ease, the proposed curve is plotted and the regions of valid and invalid points are marked. The DPI tool accepts all of the commands with points only in the valid region (second and fourth quadrants) and rejects all commands with at least one point in the invalid region (first and third quadrants).

4.2.2 Contradictory Mode Detection

Use Case 4, the enabling of contradictory modes described in Section 3.6, is a difficult one to protect against using heuristics only, but we attempt to do so here. We assume that some amount of static system knowledge could be programmed into the DPI tool, such as the overall penetration of DER in the connected system.

We first examine a few prerequisites for this particular attack:

- The Volt-Watt mode should be on, or the command should be requesting to turn the Volt-Watt mode on, or the system should already be injecting high amounts of active power.
- The command should be requesting to turn the Watt-VAR mode on.
- The current voltage should be less than the minimum voltage setpoint given in the Volt-Watt parameters. This ensures that the system is operating at maximum active power injection.
- The Watt-VAR curve parameters should be such that for maximum active power injection, there is reactive power absorption higher than a certain threshold that is chosen based on the known system DER penetration levels. For example, this attack is deemed irrecoverable with maximum reactive power absorption for DER penetration levels of 48% or higher [43].

This attack is most effective if the starting operating point of the attack is such that the DER is injecting maximum reactive power. This implies that the connected system is relying on the DER to provide this reactive power input and keep the voltage stable. Losing this support, and in fact having the DER start absorbing reactive power, can be destabilizing for even lower penetrations of DER. Examining the starting point of the attack is an optional rule that could be added to the detection of this attack with the DPI tool.

If all of the criteria described are met, an alert is raised and the packet is dropped. If one criterion is not met, then the command will be allowed to pass. If the rules for this attack are not well-tuned for the system, it may be possible to get false positives or false negatives.

4.2.3 Limiting Power Factor

Limiting the power factor is another engineering control proposed in [54] that we implement here. Similar to some of the use cases proposed in Chapter 3, malicious control of the power factor was shown to drive the voltage up by injection reactive power. By monitoring the current reactive power, the DPI tool can decide if a high power factor should be allowed or not. Specifically, if the DER is already outputting at high reactive power, the power factor should be curtailed. The cutoff proposed by Johnson et al. [54] and implemented in the current version of the tool suggests that if reactive power is above 50% of nameplate capacity, the power factor should be limited by a cutoff value. It is possible, and potentially valuable, to have this be a sliding scale rather than a strict cutoff. For example, at 50% reactive power output, power factors greater that 0.7 should be rejected, and at 70% reactive power output, power factors greater than 0.55 should be rejected.

4.2.4 Tightening Ride-Through Parameters

In many of the use cases described, tight ride-through and tripping parameters had the potential to increase the impact of an attack. Additionally, these are not parameters that would be expected to change often. Thus, a command that reduces the deviation from nominal levels (voltage or frequency), or that decreases the amount of time that a ride through should last before a device trips, is a potential warning sign of an attack. The command on its own does not guarantee that an attack is in progress, but it should still be treated as suspicious.

As it stands, the DPI tool does not reject this command, but sends a special warning message to the user. In the future, this could be developed into a "threat threshold," where commands are monitored over a period of time. Each suspicious command that is sent during this time may have a threat score, and when the aggregated threat score crosses a pre-determined threshold, the operator will receive a high-priority alert and future suspicious commands will be blocked. The aggregate threat score could be computed across many distributed devices in order to better detect an attack that targets multiple DER, thus increasing the chance for a higher impact event if an attack occurs.

4.2.5 Disabling DER

Like the previous case, a command that turns off the DER is not necessarily an indicator of an attack, but it is a suspicious event. In most applications, there will be control functions that can curtail power output from DER as needed without the need to turn them off via the communications interface. The shutdown should be viewed as suspicious, and if combined with the shutdown of many other devices, may warrant a high-priority alert and dropping any future incoming suspicious commands until the commands are verified to be legitimate.

4.3 Limitations of DPI

DPI can provide mitigations against specific cyber-physical attacks, but it does not protect against all attacks. As a rule-based approach, it is limited to the rules that are defined by a developer. If an adversary sends a command that does not meet any of the rule-based criteria for an attack, then it will evade detection. This motivates the need for a comprehensive study on combinations of modes that could be destabilizing.

This tool in particular is limited by the information available to it. The tool has access to the proposed command, the local state information, and the current configuration information of the DER. There is potential for more generic system information, such as the DER penetration level, to be programmed in as well. Even though this is sufficient information to make informed decisions, it is possible that with more information the DPI tool could detect a wider range of potential attacks.

We described some commands that were deemed "suspicious," but not necessarily adversarial. There is subjectivity to deeming commands suspicious, or aggregating the total number of suspicious commands that have been received by DER. Further investigation will be required to tune cutoffs or define levels of suspiciousness.

4.4 Future Development

The DPI tool is currently in early stages of development. There is potential for this tool to be developed from a simple rule-based tool to something more state-aware and dynamic.

One potential improvement is to make the tool more state-aware by giving it access to data collected from different points in the system rather than just at the PCC. This would allow it to make decisions based on a better understanding of the current status and the expected change from the proposed command.

We discussed one way to make this a distributed DPI tool in the previous sections. Commands can be monitored for a "suspiciousness" indicator, and this indicator can be reported back to a central node. If the net suspiciousness indicator passes a threshold, an alert can tell endpoints to stop accepting any commands that may be suspicious. Another way to formulate this a distributed intelligence tool is to have every command received by an endpoint checked by a central monitor. This method would incur heavy latency penalties, which may not be tolerable. To counteract this, a heuristic checking process may be deployed. On "high risk" nodes, perhaps 80% of commands would be checked by the monitor. On "low risk" nodes, perhaps only 10% of commands would be checked. This provides some additional security without compromising too much speed.

To make the decision-making even more robust, the tool would ideally be able to run a simulation with the changes proposed by the new command to decide if it is adversarial. Even more robust would be to run simulations under different potential grid-stress events to detect whether the command is a delayed attack, which may only come into effect under certain conditions. An example of this is the malicious Volt-VAR settings. As long as the voltage is near nominal, the response from Volt-VAR mode will be small, but if there is a large enough deviation initiated somewhere else in the system, the malicious Volt-VAR mode behavior will drive the voltage even further from nominal levels.

Even with real-time simulation capabilities, it is infeasible to run simulations for each new command that is sent. Real-time simulations still take valuable time from the executing the command, but under most scenarios, the command will be legitimate and potentially needed. Running long-term

simulations or simulations under grid-stress events would be even costlier. On top of that, the computing resources required to run high fidelity simulations are significant and not likely feasible to deploy on network endpoints.

To take advantage of the benefits of simulations, many representative scenarios with many possible commands could be run offline. When a new command is received in real-time, the inspection tool can pick from this offline database the scenario that the proposed command and current state conditions most closely align with and look up the result from that simulation. If the simulation is stable, the command is accepted and forwarded to the DER controller. If the simulation passes some threshold for instability, the command is dropped and an alert is raised.

4.5 Related Work

The previous section described a deep packet inspection tool for prevention or early detection of an active attack on the communications interface of a DER. Engineering controls that consider the power system effects of a command are not the only measures that can add security.

4.5.1 Protocol Security

Industrial protocols are typically not designed with security in mind. However, there are security features that can be designed for protocols or added on top of existing protocols. A detailed analysis of certificates and tokens used for authentication was performed and is presented in Chapter 6.

Cryptography has been proposed to protect the confidentiality of data. However, there are strong demands for low latency communications in power system communication networks, and adding cryptography is known to slow things down [55]. Work has also been done to address the latency issues and make cryptographic solutions feasible for large-scale deployment on devices with low resources [56]. Adding cryptography would also complicate the deployment of a DPI tool like the one described above. The endpoint monitor would need to have access to the crytopgraphic keys in order to read the incoming command and perform the analysis.

Deploying cryptographic solutions presents logistical issues as well. There

is a strong need in power systems for backwards compatibility as new systems and technologies are never replaced entirely at the same time, but rather rolled out over time. The adoption of IEEE-1547 presents a good opportunity to roll out cryptographic protocols for use with DER since the requirements of the standard will require changes to newly produced DER communication interfaces anyway. If it can start somewhere, the adoption of cryptographic protocols may spread to other parts of power systems. Securing certain parts of a network does little good if there are ways to circumvent the secure protocols and use insecure ones, as demonstrated in Chapter 6. However, no improvements can be made if the work does not start somewhere.

4.5.2 FDI Detection

There has been a lot of work around detection of FDI attacks. Perturbation analysis is one good way to detect if SCADA data has been compromised [57, 58, 59, 60]. This work could be extended from defending state estimation to defending against attacks specific to DER. The premise is the same: The compromised information is used to inform operational decisions, and the adversary picks the injected data to specifically force the control and operation in a certain, potentially hazardous direction. The scope would be smaller compared to the work done on distribution or transmission systems, and would instead focus on the local network the DER was connected to. An interesting approach was proposed by Jhala et al. to use probing to detect FDI attacks against systems with high penetrations of DER, but the approach is not necessarily focused specifically on the compromise of DER data [61]. A defense technique more specific to DER, namely solar, is identified by Jafarigiv et al. [62]. This work is specifically in response to FDI attacks targeting smart meters, but could be extended to a broader category of attacks.

4.5.3 Network Segmentation

Network segmentation is a way to separate logical subnetworks and prevent an adversary from being able to access all devices on a network simultaneously. This is particularly valuable since one of the big threats to DER

cybersecurity is that of a simultaneous attack on multiple DER that, in aggregate, has a destabilizing effect on the system. Network segmentation is proposed as a best practice for cybersecurity of DER by researchers [54].

4.5.4 Anomaly Detection

Most existing work focuses on potential attack vectors and best practices for proactive cybersecurity, but there are a few papers that discuss attack detection and mitigation. A tool to flag anomalous smart inverter behavior has been developed [63]. This tool also proposed a cyberattack detection mechanism based on anomaly detection using data from geographically separated DER. This work does not discuss a method for attack prevention. A similar approach has been used to detect FDI attacks that evade static bad data detection schemes [64]. A different threat model has also been studied in which the attacker has control of a photovoltaic system and changes the output to manipulate voltage. In this work, an anomaly detection system classifies good and bad behavior despite the normal unpredictable output of solar generation [65]. Another recent work describes an online unsupervised learning method to detect abnormal communications for photovoltaic systems [66]. This work uses not message content information, but rather information from the header as well as parameters like the length of the connection, as features to train the network. This tool may not work well for attacks that have compromised an engineering workstation and send commands that mimic the type of commands that could be sent during normal operations.

CHAPTER 5

POTENTIAL CONSEQUENCES OF A SUCCESSFUL ATTACK ON STORAGE DEVICES

In the previous chapters, we showed how the capabilities now required under IEEE 1547-2018 could be misused in certain combinations to create adverse power effects on the connected system for any generic DER. Now, without reference to any particular standard, we discuss a wider range of possible consequences, but with a focus on grid-scale batteries rather than generic DER.[1] Batteries are chosen for this analysis because of their inherent ability to charge and discharge active and reactive power. The increased capabilities gives the adversary a wider range of cyber-physical security scenarios to consider. Also, unlike solar or wind assets, batteries are dispatchable on command, subject to the state-of-charge. The variability of wind and solar is interesting to study for other purposes, but the dispatchable property of batteries suits them well for security analysis.

The analysis is broken up into categories of impact: Grid consequences, battery consequences, and economic consequences. The impact to power stability in a connected grid system is studied for systems with a compromised battery. Battery degradation and safety hazards are discussed. Finally, we consider the economic impacts of a cyberattack manipulating a grid-scale battery.

[1]The work in this chapter was performed as part of the author's role as a Graduate Fellow for Idaho National Laboratory. This work was performed under the auspices of the U.S. Department of Energy by the Idaho National Laboratory under Contract DE-AC07-05ID14517. The work was supported by the U.S. Department of Energy's Grid Modernization Laboratory Consortium.
The work in this chapter has been submitted for publication to the *Energies* journal special issue: "Cyber Physical Power and Energy Systems" [67].

5.1 Grid Consequences

Any effects of a cyberattack on a grid-scale battery will depend on the configuration and capabilities of the battery and inverter, as well as the configuration of the electrical elements around the battery. If the battery is the primary local source of injecting or absorbing power, any manipulation of these functions will have a greater effect than if there is a lot of inertia in the system from other sources. Safety equipment and settings on protective relays will also affect the outcome of any attack. Relays or breakers that are programmed to trip after narrow bounds are exceeded will create different effects than settings that are tolerant of a larger range. One is not necessarily more damaging than the other, but rather the effects depend on the resilience and the resilience goals of the system. Causing a device to trip after narrow bounds are exceeded may create more problems by creating a sudden change in load or generation, or it may stop the battery under attack from continuing to adversely affect the connected system.

The impacts described below consider the worst case scenarios to demonstrate the possibilities. However, not all systems will be configured to make certain attacks feasible, or the feasible impact of any battery output may be small enough that attacking the storage device may not cause measurable instability in the system. A detailed analysis of DER penetration levels needed to cause instability under certain attacks is presented in previous work [43]. These scenarios are more likely to occur in isolated microgrids or smaller systems.

5.1.1 Voltage Instability

Reactive power output is often used to regulate voltage. Absorbing reactive power can help bring the local voltage back to nominal if the voltage is high, and conversely, injecting reactive power can help bring the local voltage back to nominal if the voltage is low. Historically, capacitors and load banks were used to perform these functions, but since modern battery inverters can nearly instantaneously inject or absorb high amounts of reactive power, they are useful tools for supporting local voltage. They can be even more useful in combined solar-storage systems, since distribution systems with high solar penetration are known to have high voltage issues during high energy

generation times of day [68, 69].

A grid overvoltage event can occur if the battery fails to provide reactive power support when it needs to, or if it is adversarially manipulated to drive the voltage up. The system may tolerate higher voltages for a period of time, but if the high voltage persists, the battery will likely trip off.

A grid undervoltage event can similarly occur. In this case, the battery fails to inject reactive power when it should, or it absorbs reactive power when it should not, driving the local voltage down. If the system cannot correct for these effects, the battery may reach tripping thresholds.

Directly manipulating the reactive power output of the battery is the simplest way to create voltage instability. If there is a direct reactive power output setting, an adversary could turn it off to prevent any reactive power support, or maliciously command the battery to a reactive power setpoint that is destabilizing. There may also be various reactive power support modes. These will be required for IEEE 1547 compliant devices. An adversary can turn off Volt-VAR mode or inject setpoints for the Volt-VAR curve that amplify voltage deviations rather than mitigate them.

5.1.2 Frequency Instability

Frequency regulation is another service that can be performed by a battery. Load shedding is the most common way to deal with under-frequency events, and many researchers have explored the best under-frequency load shedding (UFLS) schemes [70, 71, 72]. Similarly, generation shedding can be used to correct over-frequency events [73, 74]. Both of these mitigations come down to re-balancing the active power for a system. Since grid-scale batteries can both inject and absorb active power, they are good candidates for mitigating frequency instability. However, the same capability that makes batteries good for frequency control gives them the potential to adversely affect the frequency if they are maliciously manipulated.

If the frequency is high, the battery can absorb active power, which has the same effect as shedding generation and drives the frequency back down to nominal levels. However, if this function is disabled or if the battery is manipulated to inject active power instead of absorbing it, an over-frequency event can be created or exacerbated. If the local frequency is out of sync

with the larger system capacity or if the whole system frequency is driven upward, equipment could be damaged and many sub-systems are likely to trip. If enough load trips, the over-frequency event will be even more extreme.

Similarly, if the frequency is low, the battery can inject active power, which has the same effect as shedding load. However, if the battery instead absorbs power in this situation, that is like adding more load on the system, which will make the under-frequency event worse. If the event is extreme enough, various sub-systems may trip.

An adversary could manipulate the frequency by directly changing the active power output or by making changes to frequency support modes, if available. By directly modifying active power output commands, an adversary could set active power output to maximum injection or absorption, driving frequency higher or lower respectively. Frequency support modes could be directly disabled or manipulated to interfere with the correct functionality. An adversary can modify frequency support bands so that frequency must deviate more before corrective actions are taken. An adversary can also modify the frequency-watt curve so that there is a smaller change in active power output in response to frequency deviations. A more subtle attack would be to modify charge rates or active power ramp rates to low values so that in any scenario, the battery is not permitted to change the active power output quickly. The effect of these actions would depend on how the controller worked, what modes were available, and the robustness of the connected system.

Typically, a system with many different generation sources has enough inertia to keep the frequency within a narrow band, particularly if many of these are traditional spinning sources. However, as penetration of inverter-based generation sources, including batteries, increases, there is less physical inertia in the system, and the system may be more susceptible to frequency deviations. This is true for smaller systems like microgrids as well.

In systems with high DER penetration, frequency regulation is a harder problem to solve [75]. If the battery does not provide the expected support in an under-frequency scenario, traditional methods like load shedding must be applied to prevent the system from collapsing [76]. An adversary could potentially trigger a load-shedding event by forcing a battery charge rapidly, absorbing enough active power to drive the frequency down, a scenario that is possible in a microgrid or other system where the battery represents a large

enough portion of generation capacity.

5.1.3 Load Shedding

Load shedding was discussed in the previous section, but there are in fact a few ways in which manipulating the battery output could cause load shedding. The first is to have the battery absorb as much active power as possible. In this scenario, the battery acts as a large load itself. If this happens at a time when generation is scarce, perhaps when solar or wind are underperforming, it could force other loads to be dropped.

Another scenario where load might be shed is if the battery is set up in such a way that it is contracted to a utility to provide certain services or a certain amount of active power injection. In that case, an adversary could manipulate the commands that tell the battery how much power the utility demands. If the battery is forced to meet this contract with manipulated values, it is possible that the battery power would all go to the utility, and it would not be able to supply local loads.

Theoretically, any of the previous scenarios in this section could also cause load shedding. If the grid disturbances are severe enough, and if they are exacerbated by an attack, then protective relays may trip, disconnecting loads from any power source. In the right scenario, the disconnect of these loads could further exacerbate an event, causing cascading failures.

5.1.4 Islanding

Many modern inverters have the ability to operate in a grid-forming mode. In this mode, direct control of active and reactive power output is not available, but instead, an operator can set a target voltage and target frequency. An adversary could manipulate these target parameters, or the supporting parameters, including frequency droop and voltage droop settings.

A successful attack on these parameters could damage equipment that is only rated for certain voltages. It could prevent the successful formation of a dynamic scheduled island. It could also interfere with the ability of the battery to support in black start scenarios. Taking away any of these functions would greatly reduce the resiliency that is provided by batteries.

At this time, it is uncommon to have a significant islanded system that is primarily powered by inverter-based devices. From a risk perspective, the likelihood of an attack on this configuration is low. However, it is important to still consider these cases, particularly if these microgrid configurations support critical operations.

5.2 Battery Consequences

In addition to the effects on the connected system, the effects of a cyberattack on the battery itself can be studied. There has been less active research in this area, but valuable insight is gained from studying the potential failure modes of the battery, and by considering cyberattacks on the batteries of electric vehicles (EVs), which share much of the same battery technology with grid-scale batteries.

There are many different chemical makeups of batteries for grid-scale storage, but lithium-ion (Li-ion) is the most common. It was developed in the 1980s, and the first commercial Li-ion battery was released in 1991 [77]. Li-ion batteries are popular because they can operate at high cell voltages and they have a low self-discharge rate. They are efficient in that they have a high power density by volume, and high specific energy and energy density [77]. These properties make Li-ion batteries well suited for deployment in electric grids. However, care must be taken to operate the batteries within their parameters for voltage, temperature, and current to ensure that there is no damage to the battery cells while charging or discharging. If they are not operated correctly, cell damage can reduce the lifespan of a battery, which is costly for electric systems. In the most extreme case, cell damage can lead to thermal runaway or fire.

5.2.1 Cell Degradation

Batteries will naturally degrade over time, and in fact, Li-ion batteries are chosen for their energy density, not for their resilience over time. Two main processes account for cell degradation [78]. First, growth of the solid electrolyte interphase (SEI) layer can cause degradation. The SEI layer grows as a result of solvent reduction at the anode-electrolyte layer. This process

consumes lithium ions, which decreases the amount of active lithium ions and reduces the capacity of the battery. Second, lithium plating can cause degradation by similarly creating a loss in capacity. It can also increase the risk of internal shorts, which could lead to system failure. The extent of lithium plating is controlled by the electochemical potential for lithium deposition.

Degradation of batteries is hard to measure, but metrics like the change in internal resistance can be used to help analyze damage, as discussed by Sripad et al. [78]. The rise in internal resistance is estimated using the increase in the thickness of the SEI layer. Degradation is affected by variables including temperatures, state-of-charge, pack size, and age of the pack. Studies evaluated by Sripad et al. showed that damage occurs faster at higher ambient temperatures [78]. However, cyberattacks are more effective on batteries in lower ambient temperatures because these batteries have thinner SEI layers to start with. They also found evidence that attacks on fully charged battery packs would cause more long-term damage.

From a cybersecurity perspective, battery degradation can be induced by overcharging or overdischarging the battery. An attack that aims to overcharge the battery causes an increase in the SEI growth rate and an increase in internal resistance. One study found that an attack that overcharges the battery by just 0.4 V after full SOC is reached has the potential to shorten the lifetime of an EV battery to about 200 days [78]. In an extreme attack, if enough lithium plating occurs, thermal runaway could occur. While this attack was demonstrated for EVs, not grid-scale batteries, a different attack path that causes overcharging would have the same effects on the battery. If an attacker can modify the upper cut-off voltage, the battery will be charged at a higher voltage than what it is rated for, causing overcharging. This is not typically something that can be modified through a standard controls interface, but rather something that would be exploited through firmware attacks or supply chain attacks.

Conversely, if the lower voltage cut-off voltage is decreased, the battery pack can be overdischarged. When overdischarge occurs, the anode potential increases abnormally and the SEI layer decomposes. This is followed by the dissolution of copper ions from current collectors, opening the possibility of internal shorts [79, 80, 81]. Copper dissolution can begin within hours but depends on the amount of power drawn during overdischarge. Eventually, metallic copper is deposited [82]. Another risk to be aware of is that Li-ion

batteries connected in series are more likely to be overdischarged [82]. The consequences of an overdischarge could range from internal shorts to thermal and safety issues.

Researchers have shown that battery-draining cyberattacks on EVs are possible, but these exploits relied on attack paths specific to the car application, and would not transfer directly to power grid applications.

One attack drains the EV battery by using the wake-up function of a parked EV, then issuing commands to turn on lights, air conditioner, wipers, and more to drain the battery [83]. The researchers took advantage of the fact that signals and messages, particularly the wake-up message, were designed to be simple in order to conserve power. The simplicity of the messages made them easier to spoof. For a grid application, an adversary would have to find a legitimate way to communicate with the battery and command it to discharge power. In addition to protocol security and other measures, the attack would be more difficult in this scenario since the grid is always on, and there will always be sensors monitoring the battery output. It is more likely that this sort of attack would be discovered before severe damage was done.

In another study, researchers investigated the entire overdischarge process by charging a Li-ion cell [82]. They observed a significant voltage plateau at approximately -12% SOC, and an internal short was detected when passing this voltage step. This suggests that an overdischarge of just -12% SOC is needed to cause short circuiting and permanent damage. The researchers also observed a sharp decrease in resistance at the beginning of the internal short circuit. After recharging samples that experienced an internal short, the cells displayed significant self-discharge. Cells that were overdischarged to a SOC of less than -14.5% could not be fully recharged to their nominal value.

5.2.2 Thermal runaway

In the most extreme case, overcharging can force cell temperature above a critical temperature, above which the increase in temperature is irreversible. This is called thermal runaway. Sometimes smoke may be seen exiting the battery pack, which is gases emitted from the degradation reactions. These

gases may cause cell ignition and combustion, starting a battery fire [84]. There is some heat generation inside the battery caused by normal charging and discharging, but if undesirable side reactions occur, this heat can rise to unsafe levels.

A fire study by the National Fire Protection Association on a commercial-scale Li-ion battery found that thermal runaway could be induced by high temperatures but did not find evidence of explosions [85]. The thermal runaway was limited to battery cells that were in closest proximity to a burner that was installed inside the battery; other cells farther from this burner were not severely affected. This is good evidence that even if a cyberattack could cause overcharging, the safety hazards would be limited. This report also studied reported cases of ESS fires. They found very few cases to study, which is again encouraging from a safety hazards perspective.

5.3 Economic Consequences

A final category of impact to consider is that of economic consequences. An adversary could manipulate battery output within all power and safety limits, but still affect the operation of the grid and the economic impact on asset owners. The effects for two categories of asset owners are presented. The first is utility owned bulk-battery assets. The second is consumer-owned battery assets.

5.3.1 Utility-owned Assets

At the utility scale, the manipulation of services required to support independent system operators (ISO) or regional transmission organizations (RTO) can have wide-reaching impacts. Both organizations are responsible for the operation of transmission systems. They oversee both energy and ancillary service markets in the regions they govern. The following list describes services that a battery can provide to a utility and how an adversary can manipulate those services.

- **Frequency Regulation:** A battery can benefit a utility or system operator by providing frequency regulation. To block this benefit, an

adversary can turn off frequency support if that is a built-in mode, or make reactive power ramp rates very slow so that any frequency response is not effective at the necessary time scale.

- **Voltage Support:** To prevent a utility or system operator from realizing the benefits of voltages support, the adversary can turn off any reactive power modes, directly manipulate voltage as discussed earlier, or make the active power ramp rate very slow.

- **Spinning Reserves:** In order to meet sudden changes in demand, there is a requirement of a certain amount of "spinning reserves" that are ready to deliver power immediately. Using batteries at the right time, particularly in times of peak load, can reduce the demand for other sources, allowing cheaper sources to be used as spinning reserve and preventing more expensive peaker plants from needing to start up. Alternatively, since batteries can change their output from zero to full injection almost immediately, the batteries themselves can be used as spinning reserves, rather than for demand response. An adversary can prevent batteries from being used to help shave peak load or act as reserves by draining the battery and keeping it at a minimal SOC.

- **Black Start:** Recent research has discussed using distributed resources, including batteries, to perform black starts. This is a bottom-up approach rather than the traditional approach of starting big base load plants first and working outward. An attacker can prevent batteries from being useful for black start by forcing the battery to maintain a low SOC.

- **Distribution and Transmission Deferral:** Installing batteries can allow utilities to delay, reduce the size of, or completely avoid investments and upgrades to the distribution or transmission systems, which would otherwise be required to meet projected load growth in certain areas of the system. An attacker can manipulate batteries to make them appear unreliable, or send commands so they are used in a way that degrades their lifetime faster. If this occurs, it may not be economically advantageous for utilities to delay the upgrades to systems.

- **Transmission Congestion Relief:** During peak demand times of the day, one of the challenges is to get power from where it is produced to where it is consumed. ISOs charge utilities higher rates to use congested transmission corridors during these times of day. Installing battery capacity downstream of these corridors can serve more local load and reduce congestion on the transmission lines. If an attacker can force the battery to maintain a low SOC or reach a low SOC at the peak demand times of day, the utility may incur increased costs from transporting more power on the transmission corridor.

5.3.2 Consumer-owned assets

The electricity market is complex, and there are many ways that consumers can receive discounts or benefits from installing DER and also ways that they can be penalized for mismanagement of the DER. The following are properties that can benefit consumers when they have batteries installed and descriptions of how attackers can take that benefit away.

- **Time-of-Use Bill Management:** In some regions, customers may be billed different rates for electricity that is consumed at different times of the day. Batteries can reduce the customer's bill by charging during low-cost times of the day and discharging to serving local load at high-cost times of the day. If the adversary prevents the battery from being used for economic efficiency, the customer's savings will decrease. The adversary could even increase a customer's bill by forcing the battery to charge during peak cost times of day.

- **Increased DER Self-Consumption:** In some regions, such as Hawaii, there are regulations prohibiting or limiting power exported form a residential home with DER (non-export rules) [86, 87]. In these locations, the primary generation source, such as wind or solar, is typically installed with a battery so that when renewable generation exceeds the power consumed by the residence, the battery can be charged rather than curtailing the generation output. The battery can later be discharged when renewable generation is low. In the worst case, an attack that prevents the battery from charging when renewable generation is high may cause the residence to violate non-export rules. Even

if the generation is curtailed, the customer will have to pay for utility electricity later that could have otherwise come from the battery.

- **Demand Charge Reduction:** Utilities charge customers for the total amount of energy (in kilowatt-hours [kWh]) that they use in each billing period. However, for customers that have peak power loads above a certain threshold, utilities will often include a "demand charge" in their billing structure, which is proportional to the peak power demand of the customer over the billing period. Batteries can be discharged at periods of peak load to offset the power imported from the utility and reduce the demand change. This also requires that batteries be charged during lower load periods. If the adversary prevents the battery from performing this function, the cost savings of having the battery will be forfeited.

- **Backup Power:** Batteries with grid-forming capabilities can provide backup power if the main electric grid is unavailable. To take advantage of this value, the battery needs to have sufficient stored energy when it is needed for backup. If the adversary forces the battery to stay at a low SOC, the value of having the battery as backup is eliminated. This translates into actual costs when considering the value of load lost or productivity lost.

CHAPTER 6

CASE STUDY: GRID-SCALE BATTERY

While many proposals address cyber-physical risks associated with DER, and a few even discuss batteries specifically, this case study is the first to perform a comprehensive analysis of the cyber-physical security of grid-scale batteries. In this study, experiments examine the security features that can be added to communications to better protect controls against adversarial manipulation; furthermore, we demonstrate a selection of the physical consequences that can occur if the adversary is successfully able to manipulate the control channels.[1]

6.1 Threat Model

In this case study, the threat model assumes that the adversary has man-in-the-middle (MitM) capabilities and the intention is to spoof commands from the AEPS to the battery controller. The attack path prior to this point is not specified. This malicious command attack has the potential to cause most of the Grid Consequence and Economic Consequence outcomes described in Sections 5.1 and 5.3. Battery hardware consequences are still of interest, but since this area has not been well studied and would appear to require more advanced adversarial capabilities, we do not focus on that in this case study.

For the communications study, the threat model assumes that the attacker is able to spoof syntactically correct messages that impersonate the AEPS operator and are sent to the battery controller. We examine success of the

[1]The work in this chapter was performed as part of the author's role as a Graduate Fellow for Idaho National Laboratory. This work was performed under the auspices of the U.S. Department of Energy by the Idaho National Laboratory under Contract DE-AC07-05ID14517. The work was supported by the U.S. Department of Energy's Grid Modernization Laboratory Consortium.
The work in this chapter has been submitted for publication to the *Energies* journal special issue: "Cyber Physical Power and Energy Systems" [67].

attack if different authentication and integrity security features are used.

For the cyber-physical outcomes study, the threat model assumes that the attacker is able to execute a successful MitM attack, or has performed reconnaissance, gathered access credentials, and is able to use an engineering workstation by pretending to be a legitimate user.

FDI attacks are out-of-scope for this case study; only command injections are considered. FDI attacks are a valid concern to be addressed, but they are more complex, requiring more advanced capabilities, which reduces the likelihood that they will occur. Also out-of-scope are insider threats, supply chain threats, or side-channel threats. An insider threat makes the communications study irrelevant as the insider would have access to proper credentials. The assumption is that the battery hardware can be trusted and that the controller firmware operates as intended.

6.2 Methods

A large grid-scale battery was configured to work in both on-grid and off-grid modes. It was also connected to a load bank and a solar emulator.

We evaluate two aspects of the cyberattack. First, we evaluate the security properties that can be added to communications to make it harder for an adversary to interface with a controller. Second, with these security features disabled, we examine the physical and electrical effects of potentially malicious commands.

6.2.1 Communications Security

Many grid-scale batteries are designed to function with multiple protocols in order to maximize compatibility. Most industrial protocols used in power systems, such as Modbus, DNP3, or versions of CAN, do not provide security features like authentication or encryption. Security was not a concern when these protocols were designed, but even as recognition of the need for industrial security grows, they continue to be deployed widely in practice for convenience and to ensure backwards compatibility with other devices. The transition to secure communications cannot be made unless security features are made available, and eventually required, but in the meantime some

devices are equipped to communicate both securely and insecurely.

We test whether the battery controller can respond simultaneously to requests sent via different protocols. We request data for logging purposes via a authenticated protocol, and test the response to simultaneous commands sent that impersonate the AEPS controller but communicate via an unsecured protocol. We verify if the unauthenticated commands are accepted by the controller by monitoring the data collected via the secure protocol. This test is not meant to examine the security of one protocol over the other, but rather to demonstrate that even when secure communications are available, there may be ways for an adversary to bypass the security without learning necessary credentials.

Next, we examine two individual security features that can be added to industrial protocols: token authentication and certificate authentication. When the AEPS uses a protocol with tokens, the server, the battery controller, is authorized to give access (read or write) to certain resources based on the token. For the client to verify the authenticity of the server, certificates are used. A client verifies a server according to its certificate, and the server identifies the client according to the client certificate, which is known as mutual-authentication. While both of these are authentication features, the distinction is that tokens grant a level of access to certain resources so that the server can trust the client, whereas certificates verify identities, typically so that the client can trust the server.

6.2.2 Controller Interface Security

If we assume that the adversary can send a message that is accepted by the battery controller, we want to know what the cyber-physical impact will be, specifically how the adversary can misuse functionality available through the controller to cause physical and measurable effects on the connected power system. We also examine what can be done to mitigate the effects of adversarial commands. In this case study, we explore the misuse of two common modes for battery controls — active or reactive power output setpoints and Volt-VAR mode setpoints — and we show how engineering controls can protect against the most damaging effects.

The active and reactive power setpoints attack tests the ability of an ad-

versary to directly modify the active and reactive power output of a battery. In addition to general manipulation of the output, we test whether an adversary can send commands that are outside of battery limits or documented capacity.

The Volt-VAR setpoints attack tests the ability of an adversary to modify the points that define a Volt-VAR support curve. Typically, when this mode is enabled, the curve defines a reactive power output in response to current local voltage. When voltage is low, the battery should inject reactive power. When voltage is high, the battery should absorb reactive power. We test both normal and abnormal Volt-VAR setpoints and measure the effects on local voltage.

For these cyber-physical attacks, we carefully monitor the self-reported status, the alert logs, and the actual behavior of the device. We compare device-reported outputs with measurements collected independently on a separate power meter. The purpose of the monitoring is to determine the severity of the attack and examine the data for indicators that may alert an operator to an attack in progress.

6.2.3 Experimental Setup

The programs to interact with the controller were custom developed in Python for this project. The controller interface for the battery has the ability to communicate via an authenticated protocol and an unauthenticated protocol. We developed an authenticated data logging tool, an authenticated controls tool, and an unauthenticated controls tool.[2] The authenticated data logger and controls program recorded data and control actions to common SQL databases. Requests sent via the unauthenticated protocol were manually logged.

The data logger requested different information at varying intervals in accordance with how often that data was expected to change. Power output data was polled at a frequency of 10 Hz. System status data was polled at a frequency of 1 Hz. Mode status, which included configuration data and was not expected to change often, was polled every 5 minutes. General

[2]The exact protocols and devices used are redacted to comply with the Idaho National Laboratory's export policy and comply with non-disclosure agreements in place about proprietary material.

system information was logged only at the start of every trial. The data was optionally logged to either an SQLite database, a PostgreSQL database, or both.

The authenticated controls program allowed the user to send commands that changed settings on the controller. Small changes to the program allowed us to turn the different security features, namely tokens and certificates, on and off. It operated via a command line interface. The unauthenticated controls program also operated via a command line interface. The purpose of this program was to test the controller's response to different protocols and to simultaneous commands via different protocols.

For our tests, a single grid-scale battery was operated in grid-following mode. It was connected directly to building power in the lab at 480 V. The building power infrastructure had the ability to act as both a source and a sink, permitting the battery to operate in both charging and discharging modes. A power meter was in place to independently monitor the battery output. The system setup is detailed in Figure 6.1.

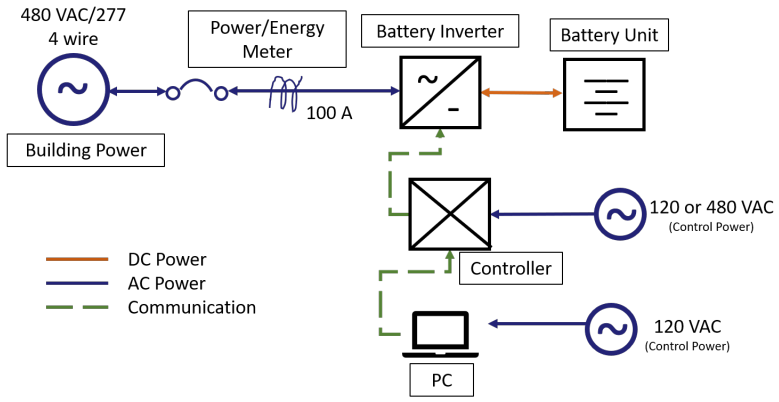


Figure 6.1: Grid-following setup for cyber-physical defense study.

6.3 Results

The tests were conducted with two separate battery and controller units to verify results.

6.3.1 Communications Security

Simultaneous Communications

As stated previously, the controller had the ability to communicate via two separate protocols. We simulated a scenario where the operator was using the secure and authenticated protocol to send commands and log data. An adversary with access to the network, but not to the credentials for the authenticated communications, injected commands using the unauthenticated protocol.

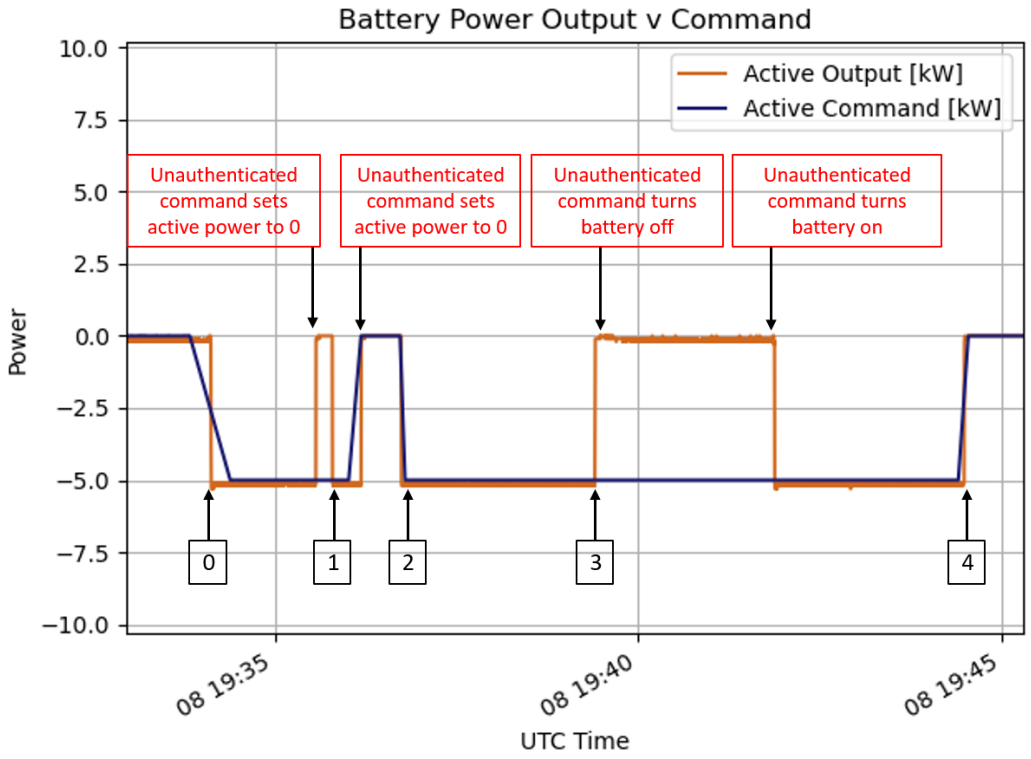


Figure 6.2: The real power outputs follow the adversary's commands even while data is being requested through the authenticated interface [67].

The commands sent by the adversary were accepted even while the authenticated data logger was also being used. The adversary sent commands to change the real power output and the battery responded by following the commands. The same was true for constant reactive power commands. The adversary was also able to send commands turning the constant real power output on and off. This shows that the controller can respond to two protocol

types simultaneously, switching rapidly back and forth between recognizing one or the other as the command source. Notably, eight total events appear in the power data logged, as seen in Figure 6.2, but only five events corresponding to commands sent via authenticated channels are seen by the event logger, as seen in Table 6.1.

Table 6.1: Event log captured via authenticated interface while adversarial unauthenticated commands were sent [67]. Indices correspond with authenticated controller events labeled in Figure 6.2.

Index	**Time**	**Mode**	**Message**
0	19:34:05.055	real power	Submitting: {"power": -5000}
0	19:34:05.133	real power	Changes accepted
1	19:35:47.070	real power	Submitting: {"power": -5000}
1	19:35:47.117	real power	Changes accepted
2	19:36:43.934	real power	Submitting: { "power": -5000}
2	19:36:44.023	real power	Changes accepted
3	19:40:03.180	real power	Submitting: {"power": -5000}
3	19:40:03.243	real power	Changes accepted
4	19:44:28.617	real power	Submitting: { "mode": "off"}
4	19:44:28.726	real power	Changes accepted

The adversarial changes can be easily detected in the power data recorded by the data logger, but the ability of an attacker to turn on and off the constant real and reactive power output is still significant. In an operational scenario, it might be difficult to quickly determine why the power output changed rapidly. The best way to diagnose this would be to monitor the parameter that states what command protocol the battery is currently following as a command source, but this could quickly be overwritten by the authenticated protocol if there was frequent communication between the battery controller and the operator.

It is worth noting that constant power output modes are only relevant if the battery is operating in a grid-following constant output mode. These commands would not be relevant if the battery was instead operating to maintain a certain SOC, for example. However, it is still noteworthy that simply using a different protocol can circumvent the protections afforded by the certificates and tokens required for the authenticated protocol.

To prevent this attack, there would need to be a method to control what protocols are allowed to interact with the controller, even if the controller has the ability to interact with many. It is theoretically possible to disable

the unauthenticated protocol by default and only allow it to be used if the owner specifically requests it and enables access. Otherwise, the authenticated protocol must be used. This type of requirement is uncommon due to the prevalent use of insecure protocols in power systems, but it may be necessary in the future. Another simple way to do this would be to have all the incoming traffic pass through a firewall that only allows packets through if they are a type that the operator approves for the destination of the battery controller.

The danger of having both protocols enabled is that it provides a false sense of security. Operators may believe that they are protected from command spoofing since they are using secure communication protocols without realizing that a different, insecure protocol can be used simultaneously by an adversary.

Protocol Security Features

The addition of any security features is an improvement on the traditional insecure industrial protocols used in power grid and grid-scale battery applications, as long as it does not lull the user into a false sense of security. In this test, the focus is on evaluating the level of additional security that was provided by certificates and tokens. First, we ensured that both data reads and data writes worked as expected when both tokens and certificates were implemented correctly in the authenticated controls interface.

Tokens are intended to ensure that a client can only access resources for which they are approved. We test their functionality by using incorrect tokens and by excluding them from messages. We changed a single bit of the token and attempted to send both read and write requests. These requests were denied. The controller returned error messages, indicating that valid tokens must be used.

Next, we attempted to send both read and write requests with no token included. Write requests were denied and an error message returned. However, read requests were successful without the token. This suggests tokens can protect against adversarial command-spoofing attacks, assuming the adversary does not have access to the token. Although the read requests without the token were successful, it is unlikely that the information they would have access to would give them much more information about the system than

what they already knew if they were in a position to intercept the messages. We reintroduced the correct token and ensured everything was working properly before proceeding to the next test.

Certificates are intended to verify identities. As in the previous test, we examined the response of the controller to incorrect and to missing certificates. First, we selected the wrong certificate to send both read and write requests. If the session had already been started using the correct certificate, both the read and write requests were successful. However, if the session was just re-starting after a period of inactivity, both read and write requests were rejected. This is expected behavior for certificates. Certificates are typically used to establish trust at the beginning of a session, and often to exchange keys so that future communication can be encrypted. It is unclear how long sessions last, and this will likely be different for different manufacturers. If encryption is not used, the risk of session hijacking needs to be accounted for. We did not have the ability to parse the firmware and discover the exact mechanism for verification, but more security can be provided if sessions are limited to short durations. This experiment showed that certificates offer protections against unauthorized read and write requests. Operators should be aware of the threat of session-hijacking. If they expect certificates to provide protections, they should ensure that the system is correctly configured to provide them those protections.

We also tested the controller response when no certificate is present. Both read and write requests were denied, and an error was returned. This implies that using a protocol where certificates are required adds strong protections. However, this feature could still be evaded. Although certificates were checked by default, there was a way to configure the packets such that the certificates were not checked by the receiver. When this was done, both read and write requests were successful. When this was done, there was a warning raised informing the user that an unverified request was being made and that adding certificate verification was strongly recommended. This warning would not deter an adversary, but would only be a good reminder for a legitimate user who had unintentionally misconfigured their control program. These results essentially show that the client (command sender) was not verifying the identity of the server (controller). While in theory this does not mean much since we consider the attacker as the sender, if certificates were provided it could offer one extra challenge for attackers before they can

execute an attack.

Tokens and certificates both add security to communications interfaces, helping ensure that unauthorized users cannot access live data sent from the controller or send malicious commands to the controller. Tokens were powerful protections against unauthorized write requests. Certificates, when required for each request, were found to protect against unauthorized read and write requests. We also note that using multiple security features together, i.e. requiring both tokens and certificates, adds layers of security, making it more difficult to spoof commands without first stealing credentials.

It should be noted that although we found ways to evade some of the security features provided by the authenticated protocol, this protocol still offered better security than the unauthenticated protocol. It is still recommended to use and to require authenticated protocols if they are available as they are an improvement on traditional industrial protocols, as long as they do not lull the operator into a false sense of security. System operators should take care, though, to ensure that they are implemented correctly and that they are getting the full security protections they expect from the features of the more advanced protocols.

6.3.2 Interface Security

In this section, we examine the cyber-physical impacts of adversarial manipulation of the controller interface. This threat model is valid if the controller accepts the unauthenticated protocol from a source that appears to be valid, or if the real command source (i.e. control center) has been compromised. We assume that it is possible for an adversary to inject spoofed commands to the controller.

Real and Reactive Power Setpoints

As we demonstrated in Section 6.3.1, it is possible for an adversary to use an unauthenticated protocol to send commands changing the constant active and reactive power output while the operator's secure data logger is running simultaneously. When the adversarial commands are sent they are not logged the same way they would be if the operator's control interface had been used, but this does not mean they are totally hidden. The active and reactive

outputs can be monitored via the active and reactive setpoints parameters, the battery controller output logs, or an external meter. Even if the battery's data could be compromised, the external meter would still show the true output.

We found that the controller did not enforce the documented limits on the real and reactive power outputs. It would allow the setpoints to be chosen as an arbitrarily high value for either injection or absorption. However, physical limits still prevented the battery from entering any unsafe conditions. For example, if the battery was commanded to discharge at a rate beyond its hardware capacity, it would only discharge up to that capacity, even though the controller still reported that the setpoint was at the invalid requested value.

An example of this behavior is shown in Figure 6.3. An adversarial command set the active power setpoint to 1010 kW. The actual active power output reached a maximum of 111.5 kW, which is the documented maximum power output of the battery.

No direct safety limits were violated since the battery limited its output to the true maximum power output. However, the software did not behave as expected, and there could still be some risks here.

Volt-VAR Setpoints

A common way to regulate voltage using reactive power is Volt-VAR mode. Reactive power should be injected to increase the local voltage, and reactive power should be absorbed to decrease the local voltage. If there are no limits enforced on the Volt-VAR curve, which designates the amount of reactive power injection or absorption based on current voltage measurements, an adversary can designate an arbitrary curve that may have destabilizing effects. The potential impact of adversarial Volt-VAR curves is discussed in [54].

Figure 6.4 shows the results of experiments with the Volt-VAR curve. Nominal voltage is 277.7 V or 0.977 p.u.. Region V shows the voltage when no reactive support is provided, approximately 271 V. In Region I, a constant reactive power injection of 60 kVAR is added to mitigate the voltage depression. This brings the voltage up to approximately 275 V. This is an improvement, but it is not a dynamic response to the local voltage. In Regions II, III, and IV, the Volt-VAR mode is enabled. Region IV shows the

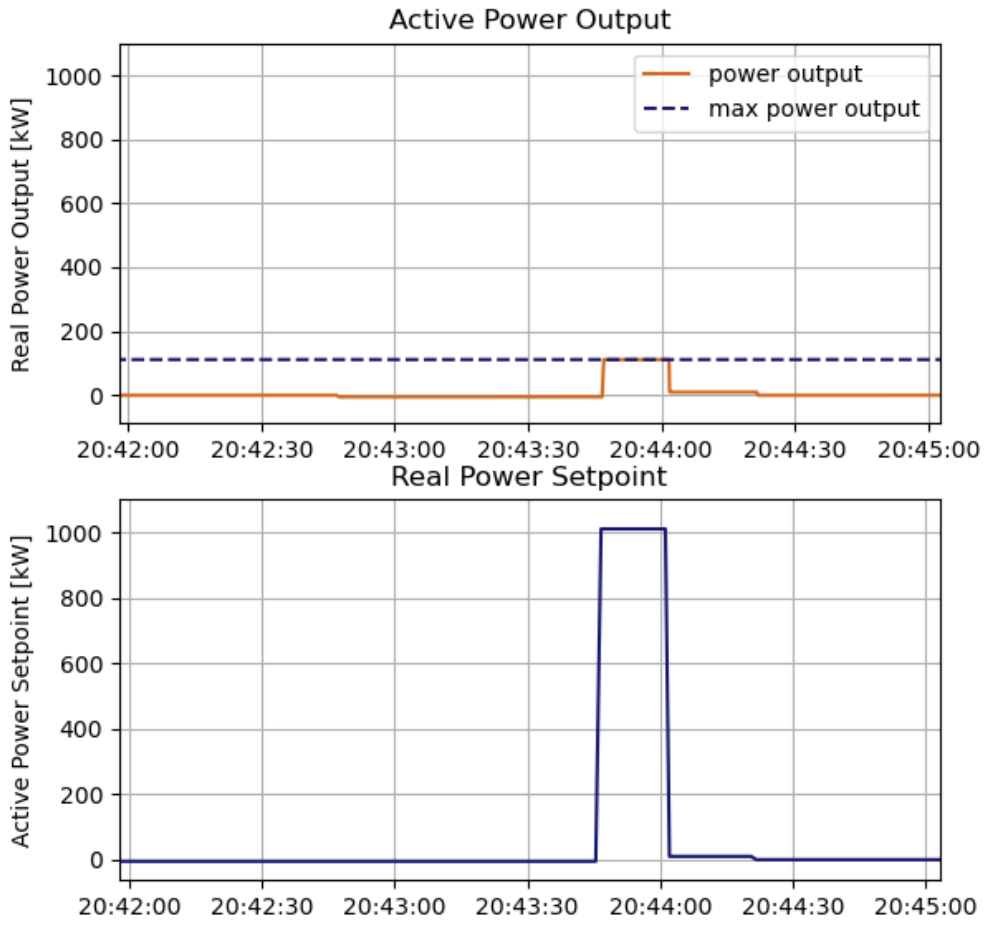


Figure 6.3: The active power output was set to 1010 kW, far above the 111.5 kW maximum power output [67].

effects of a standard Volt-VAR curve. Reactive power is injected, and the voltage is increased to approximately 275 V, which is 0.99 p.u. and indicates a good response.

Regions II and III show varying levels of adversarial input. In Region II, an adversary sends commands for an inverse Volt-VAR curve, absorbing power instead of injecting power when the voltage is low. This adversarial setting is configured to inject or absorb a maximum of 20% available reactive power. The voltage is depressed below the no-input level, down to approximately 270 V. Region III shows a more severe attack. The setup is the same, but the adversarial setpoints are configured to inject or absorb a maximum of 40%

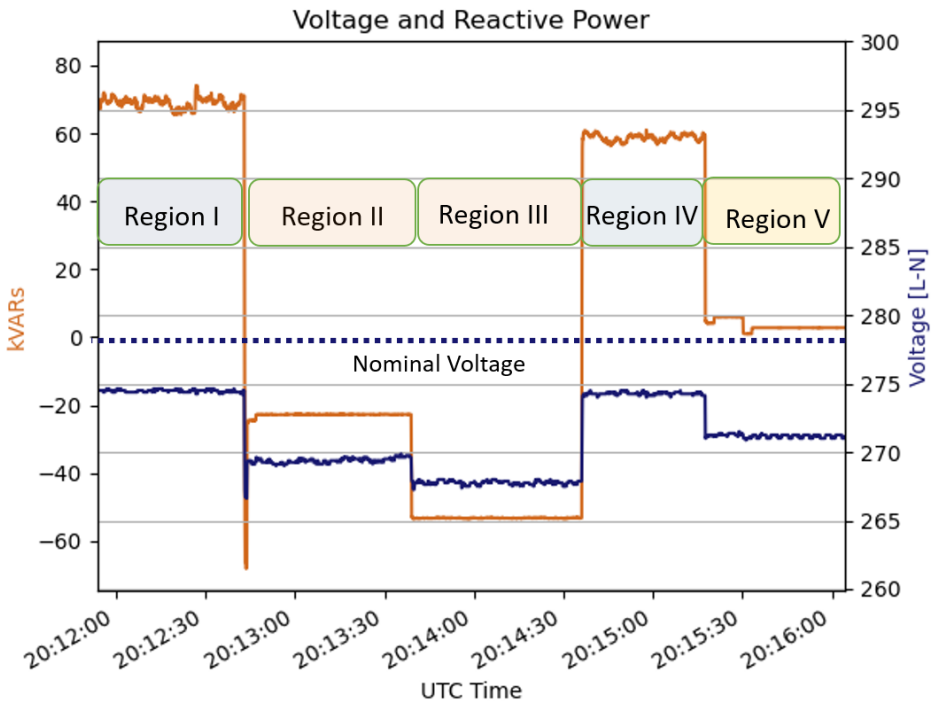


Figure 6.4: The adverse effects of a malicious Volt-VAR curve are shown [67].

of available reactive power. The voltage is depressed down to approximately 268 V, or 0.96 p.u.. This is a low enough value that safety devices might trip if the voltage remained at this level for an extended period of time. The adversarial conditions move the system farther away from the desired state. More extreme attacks are possible but not demonstrated here.

6.4 Conclusions for the Case Study

We performed a comprehensive cyber-physical security analysis of a connected battery system. From the networking perspective, the main takeaway is that authentication features like tokens and certificates do provide security benefits, event when the messages are not encrypted. If possible, authenticated protocols should be the default, and unauthenticated protocols should be disabled except where absolutely necessary.

We demonstrated command injections that resulted in a sample of the grid consequences that were discussed in Section 5.1. This experiment took

place with real hardware and real communications networks. Engineering controls can help mitigate the effects of malicious commands, but overall it is desirable to block the commands before they are accepted, which is discussed in Chapter 4.

6.5 Related Work

Most existing work that addresses the topic of cybersecurity for DER refers to the increased functionalities as one of the key features that adversaries may exploit. Different attacks that interfere with the operation of DER are shown to be feasible through hardware-in-the-loop (HIL) simulations [88]. Similar work adds a level of realism by including physical devices at different remote locations as part of their HIL simulations and studying the impact of attacks and the influence of attacks carried out at different time scales [89]. HIL simulations are also used to explore different attack paths by Duan et al. [90], but these mostly focus on attacks that result in the DER being turned off or disconnected, which is still an effective way of preventing the DER services from being used. Soyoye and Stefferud [91] assess similar risks, specifically those of functions specifically called out in California's Rule 21 Interoperability requirements, through a power electronics lens.

CHAPTER 7

CONCLUSION

This thesis has discussed the cybersecurity implications of integrating large amounts of DER into the grid. With DER penetration on the rise, a trend which is only expected to grow, there are rising concerns about the security of having so many distributed resources on the grid. In particular, the developing need for advanced control function and the communications to support these functions has broadened the attack surface for an adversary, especially compared to the traditional generation model.

A cyber-physical security analysis of the recently updated IEEE 1547 standard in the first part of the thesis reveals the potential for adversarial combinations of modes and setpoints to create harmful and potentially destabilizing effects on the connected system. In the worst case, a simultaneous attack on multiple DER can cause them all to trip off simultaneously. This is particularly concerning for systems with high DER penetration. To mitigate the likelihood for these attacks to be successful, the author developed a DPI tool to detect incoming commands that may be malicious. This tool takes a rule-based approach, and successfully alerts on the most threatening commands and sends warnings for suspicious commands.

The second part of the thesis focuses specifically on grid-scale storage devices due to their inherent ability to inject and absorb power. This built-in range of functionality and direct dispatchability makes batteries the most interesting inverter-based DER to study from a security perspective. A range of potential consequences of a cyberattack on a battery are explored according to the categories of grid stability impacts, battery hardware impacts, and economic impacts. Potential attacks that could result in these consequences are described. Next, a case study is performed with a real grid-scale storage device and networks. This adds a level of realism not achieved by most existing work. The cybersecurity properties of the battery are investigated, both from a network security perspective and a cyber-physical impacts per-

spective. Best practices and useful security features are highlighted.

Within the last ten years, DER penetration and capabilities have grown so much that there is need for cybersecurity solutions specific to DER. This thesis explores the considerations from a cyber-physical perspective, taking into account networks, communications, and attacker capabilities, as well as the physical impacts of feasible attacks. More work is needed to develop robust mitigation tools and generate awareness of best practices for managing DER, but this thesis serves as a good starting point for anyone who wishes to understand the threats and impacts.

REFERENCES

[1] "ICS cybersecurity year in review 2020," Dragos, Inc., Tech. Rep., 2020. [Online]. Available: https://hub.dragos.com/hubfs/Year-in-Review/Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf

[2] M. E. Beatty, S. Phelps, C. Rohner, and I. Weisfuse, "Blackout of 2003: Public health effects and emergency response," *Public Health Reports*, vol. 121, no. 1, pp. 36–44, 2006.

[3] B. Dakss, A. Siese, A. Sundby, and J. Carissimo, "Texans face drinking water shortage as power grid returns to normal," CBS News, Feb. 2021. [Online]. Available: https://www.cbsnews.com/live-updates/texas-drinking-water-power-grid/

[4] "Presidential Policy Directive – critical infrastructure security and resilience," PPD 21, Feb. 2013.

[5] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid: Defense use case," E-ISAC, Tech. Rep., Mar. 2016.

[6] "Crashoverride: Analysis of the threat to electric grid operations," Dragos, Inc., Tech. Rep., June 2017.

[7] "Ukraine power cut 'was cyber-attack'," BBC News, Jan. 2017. [Online]. Available: https://www.bbc.com/news/technology-38573074

[8] "Threat analysis: Industrial control system technical report: Dealing the with the threats posed by Triton / Trisis destructive malware," Accenture Security, Tech. Rep., 2018.

[9] FireEye Intelligence, "TRITON attribution: Russian government-owned lab most likely built custom intrusion tools for triton attackers," 2018. [Online]. Available: https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

[10] "TRISIS malware: Analysis of safety system targeted malware," Dragos Inc., Tech. Rep., 2017.

[11] U. J. Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, "Ransomware threat and its impact on SCADA," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. IEEE, Jan 2019.

[12] E. Goncharov, "ICS threat predictions for 2021," Kaspersky Lab, Tech. Rep., 2020.

[13] W. Schwab and M. Poujol, "The state of industrial cybersecurity in 2018," Kaspersky Lab, Tech. Rep., 2018.

[14] "Ransomware shuts gas compressor for days in latest U.S. energy infrastructure attack," JWN Energy, 2019. [Online]. Available: https://www.jwnenergy.com/article/2020/2/19/ransomware-shuts-gas-compressor-days-latest-us-ene/

[15] "Assessment of ransomware event at U.S. pipeline operator," Dragos, Inc., 2020. [Online]. Available: https://www.dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/

[16] J. Umawing, "Threat spotlight: the curious case of ryuk ransomware," Malwarebytes Labs, 2019. [Online]. Available: https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/

[17] B. Sobczak, "First-of-a-kind U.S. grid cyberattack hit wind, solar," E&E News: EnergyWire, Oct. 2019. [Online]. Available: https://www.eenews.net/stories/1061421301

[18] B. Sobczak, "Report reveals play-by-play of first U.S. grid cyberattack," E&E News, Sept. 2019. [Online]. Available: https://www.eenews.net/stories/1061111289

[19] D. J. S. Cardenas, A. Hahn, and C. C. Liu, "Assessing cyber-physical risks of IoT-based energy devices in grid operations," *IEEE Access*, vol. 8, pp. 61 161–61 173, 2020.

[20] "Distributed energy resources technical considerations for the bulk power system," Federal Energy Regulatory Commission, Tech. Rep. Docket No. AD18-10-000, Feb. 2018. [Online]. Available: https://www.ferc.gov/sites/default/files/2020-05/der-report_0.pdf

[21] "Distributed energy resources rate design and compensation," National Association of Regulatory Utility Commissioners, Tech. Rep., Nov. 2016. [Online]. Available: https://pubs.naruc.org/pub.cfm?id=19fdf48b-aa57-5160-dba1-be2e9c2f7ea0

[22] "The integrated grid: A benefit-cost framework," Electric Power Research Institute, Tech. Rep. Report No. 3002004847, Feb. 2015.

[23] N. Sadan and B. Renz, "New DER communications platform enables DERMS and conforms with IEEE 1547–2018 requirements," in *2020 IEEE/PES Transmission and Distribution Conference and Exposition (T D)*. IEEE, 2020, pp. 1–5.

[24] R. Walling, "Revision of IEEE standard 1547: The background for change," in *TechSurveillance*, National Rural Electric Cooperative Association, Nov. 2016.

[25] "HB 623 HD 2 Relating to renewable standards," House of Representatives, Twenty-Eighth Legislature, State of Hawaii, 2015.

[26] "SB-350 Clean energy and pollution reduction act of 2015," Senate, State of California, 2015.

[27] Associated Press, "New York climate plan sets 30-year goal for 100% renewable energy," *Los Angeles Times*, Jul. 2019.

[28] "DSIRE detailed summary maps," NC Clean Energy Technology Center, 2020. [Online]. Available: https://www.dsireusa.org/resources/detailed-summary-maps/

[29] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*. IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003), IEEE, 2018.

[30] K. Collardson and A. Bingham, "California's rule 21: A quick guide on inverter compliance by models and manufacturer," BayWa r.e., June 2020.

[31] D. C. Parsons, "Interconnection of distributed energy resources in Hawaii," Hawaii Public Utilities Commission, May 2019.

[32] B. M. Buchholz and Z. A. Styczynski, "Communication requirements and solutions for secure power system operation," in *2007 IEEE Power Engineering Society General Meeting*. IEEE, 2007, pp. 1–5.

[33] *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*. IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010), 2012.

[34] *IEEE Standard for Smart Energy Profile Application Protocol*. IEEE Std 2030.5-2018 (Revision of IEEE Std 2030.5-2013), 2018.

[35] *SunSpec Modbus*. SunSpec DER Information Model Specification, SunSpec Alliance, 2021. [Online]. Available: https://sunspec.org/wp-content/uploads/2021/02/SunSpec-DER-Information-Model-Specification-V1-0-02-01-2021.pdf

[36] W. Yu, Y. Xue, J. Luo, M. Ni, H. Tong, and T. Huang, "An UHV grid security and stability defense system: Considering the risk of power system communication," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 491–500, 2016.

[37] L. Chen, S. Suo, X. Kuang, Y. Cao, and W. Tao, "Secure ubiquitous wireless communication solution for power distribution internet of things in smart grid," in *2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE)*. IEEE, 2021, pp. 780–784.

[38] G. K. Chalamasetty, P. Mandal, and Tzu-Liang Tseng, "Secure SCADA communication network for detecting and preventing cyber-attacks on power systems," in *2016 Clemson University Power Systems Conference (PSC)*. IEEE, 2016, pp. 1–7.

[39] G. Bedi, G. K. Venayagamoorthy, and R. Singh, "Navigating the challenges of internet of things (IoT) for power and energy systems," in *2016 Clemson University Power Systems Conference (PSC)*. IEEE, 2016, pp. 1–5.

[40] N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, C. Lai, P. Cordeiro, A. Hasandka, M. Martin, and C. Howerter, "Analysis of system and interoperability impact from securing communications for distributed energy resources," in *2019 IEEE Power and Energy Conference at Illinois (PECI)*. IEEE, 2019, pp. 1–8.

[41] D. Ackley and H. Yang, "Exploration of smart grid device cybersecurity vulnerability using Shodan," in *2020 IEEE Power Energy Society General Meeting (PESGM)*. IEEE, 2020, pp. 1–5.

[42] "Glossary of terms used in NERC reliability standards," North American Electric Reliability Corporation, Tech. Rep., 2021. [Online]. Available: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

[43] P. Chapagain, M. Culler, D. Ishchenko, and A. Valdes, "Stability impact of IEEE 1547 operational mode changes under high DER penetration in the presence of cyber adversary," presented at 2021 IEEE Green Technologies Conference (GreenTech), Apr. 2021.

[44] "e-mesh SCADA." [Online]. Available: https://www.hitachiabb-powergrids.com/ch/en/offering/product-and-system/grid-edge-solutions/our-offering/e-mesh/e-mesh-scada

[45] M. El-Moubarak, M. Hassan, and A. Faza, "Performance of three islanding detection methods for grid-tied multi-inverters," in *2015 IEEE International Conference on Environment and Electrical Engineering ICEEE*. IEEE, June 2015.

[46] M. E. Ropp, M. Begovic, and A. Rohatgi, "Analysis and performance assessment of the active frequency drift method of islanding prevention," *IEEE Transactions on Energy Conversion*, vol. 14, no. 3, pp. 810–816, 1999.

[47] B. Dob and C. Palmer, "Communications assisted islanding detection: Contrasting direct transfer trip and phase comparison methods," in *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*. IEEE, 2018, pp. 1–6.

[48] M. J. Mukarram and S. V. Murkute, "Comparative study on islanding detection of the photovoltaic grid connected system," in *International Journal of Engineering Research and Technology (IJERT)*, vol. 08, no. 11, Nov. 2019.

[49] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected DER devices," in *2017 North American Power Symposium (NAPS)*. IEEE, 2017, pp. 1–6.

[50] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *2019 Resilience Week (RWS)*, vol. 1. IEEE, 2019, pp. 226–231.

[51] K. Matsuzaki, N. Sawabe, R. Maeda, D. Suzuki, T. Matsuura, and H. Hamada, "Cybersecurity evaluation methodology for distributed energy resources: Industrial demonstration," in *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2020, pp. 2169–2174.

[52] *IEEE Standard Conformance Test Procedures for Equipment Interconnecting Distributed Energy Resources with Electric Power Systems and Associated Interfaces*. IEEE Std 1547.1-2020, 2020.

[53] *IEC 61850-4:2011/AMD1:2020, Communication Networks and Systems for Power Utility Automation*. International Electrotechnical Commission's (IEC) Technical Committee, 2020.

[54] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, "Power system effects and mitigation recommendations for DER cyberattacks," *IET Cyber-Physical Systems: Theory Applications*, vol. 4, no. 3, 2 2019.

[55] D. Whitehead and R. Smith, *Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions*. Schweitzer Engineering Laboratories, Inc., 2018, ch. Cryptography: A Tutorial for Power Engineers.

[56] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public key cryptography in sensor networks—revisited," in *Security in Ad-hoc and Sensor Networks*, C. Castelluccia, H. Hartenstein, C. Paar, and D. Westhoff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 2–18.

[57] M. Culler, K. Davis, and A. Sahu, "PAVED: Perturbation analysis for verification of energy data," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2019, pp. 1–6.

[58] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2014.

[59] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2017.

[60] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, 2014.

[61] K. Jhala, P. Pradhan, B. Chen, and R. Singh, "Sequential perturbation-based attack detection using DERs for unbalanced distribution system," in *2021 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2021, pp. 1–5.

[62] D. Jafarigiv, K. Sheshyekani, M. Kassouf, Y. Seyedi, H. Karimi, and J. Mahseredjian, "Countering FDI attacks on DERs coordinated control system using FMI-compatible cosimulation," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1640–1650, 2021.

[63] A. Y. Fard, M. Easley, G. T. Amariucai, M. B. Shadmand, and H. Abu-Rub, "Cybersecurity analytics using smart inverters in power distribution system: Proactive intrusion detection and corrective control framework," in *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE, 2019, pp. 1–6.

[64] K. Pan, P. Palensky, and P. M. Esfahani, "From static to dynamic anomaly detection with application to power system cyber security," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1584–1596, 2020.

[65] A. M. Kosek, "Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model," in *2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG)*. IEEE, 2016, pp. 1–6.

[66] C. B. Jones, A. Chavez, S. Hossain-McKenzie, N. Jacobs, A. Summers, and B. Wright, "Unsupervised online anomaly detection to identify cyber-attacks on internet connected photovoltaic system inverters," presented at 2021 IEEE Power and Energy Conference at Illinois (PECI), 2021.

[67] M. Culler and H. Burroughs, "Cybersecurity considerations for grid-connected batteries," *Energies*, submitted for publication.

[68] L. Collins and J. Ward, "Real and reactive power control of distributed PV inverters for overvoltage prevention and increased renewable generation hosting capacity," *Renewable Energy*, vol. 81, pp. 464–471, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0960148115001949

[69] D. Teshome, W. Xu, P. Bagheri, A. Nassif, and Y. Zhou, "A reactive power control scheme for DER-caused voltage rise mitigation in secondary systems," in *2019 IEEE Power Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–1.

[70] C. Li, Y. Wu, Y. Sun, H. Zhang, Y. Liu, Y. Liu, and V. Terzija, "Continuous under-frequency load shedding scheme for power system adaptive frequency control," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 950–961, 2020.

[71] W. Tan, C. Shen, X. Zhang, and J. Ni, "A new under-frequency load shedding scheme based on OBDD," in *2009 International Conference on Sustainable Power Generation and Supply*. IEEE, 2009, pp. 1–5.

[72] X. Xiong and W. Li, "A new under-frequency load shedding scheme considering load frequency characteristics," in *2006 International Conference on Power System Technology*. IEEE, 2006, pp. 1–4.

[73] M. N. Haque Shazon, H. M. Ahmed, and Nahid-Al-Masood, "Over-frequency mitigation using coordinated generator shedding scheme in a low inertia power system," in *2020 IEEE Region 10 Symposium (TENSYMP)*. IEEE, 2020, pp. 560–563.

[74] Zhiming Song, Yong Lin, Chen Liu, Zhenbin Ma, and Lei Ding, "Review on over-frequency generator tripping for frequency stability control," in *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. IEEE, 2016, pp. 2240–2243.

[75] P. Mahat, Z. Chen, and B. Bak-Jensen, "Underfrequency load shedding for an islanded distribution system with distributed generators," *IEEE Transactions on Power Delivery*, vol. 25, no. 2, pp. 911–918, 2010.

[76] U. Rudez and R. Mihalic, "Analysis of underfrequency load shedding using a frequency gradient," *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 565–575, 2011.

[77] Y.-S. Lee and M.-W. Cheng, "Intelligent control battery equalization for series connected lithium-ion battery strings," *IEEE Transactions on Industrial Electronics*, vol. 52, no. 5, pp. 1297–1307, 2005.

[78] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of electric vehicle battery packs to cyberattacks on auxiliary components," *CoRR*, vol. abs/1711.04822, 2017. [Online]. Available: http://arxiv.org/abs/1711.04822

[79] H. Maleki and J. N. Howard, "Effects of overdischarge on performance and thermal stability of a Li-ion cell," *Journal of Power Sources*, vol. 160, no. 2, pp. 1395 – 1402, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378775306004277

[80] H. Lee, S.-K. Chang, E.-Y. Goh, J.-Y. Jeong, J. H. Lee, H.-J. Kim, J.-J. Cho, and S.-T. Hong, "Li2NiO2 as a novel cathode additive for overdischarge protection of Li-ion batteries," *Chemistry of Materials*, vol. 20, no. 1, pp. 5–7, 2008. [Online]. Available: https://doi.org/10.1021/cm702290p

[81] H. Li, J. Gao, and S. Zhang, "Effect of overdischarge on swelling and recharge performance of lithium ion cells," *Chinese Journal of Chemistry*, vol. 26, no. 9, pp. 1585–1588, 2008.

[82] R. Guo, L. Lu, M. Ouyang, and X. Feng, "Mechanism of the entire overdischarge process and overdischarge-induced internal short circuit in lithium-ion batteries," *Scientific Reports*, vol. 6, no. 30248, 2016.

[83] K.-T. Cho, Y. Kim, and K. G. Shin, "Who killed my parked car?" arXiv:1801.07741, 2018.

[84] S. Abada, G. Marlair, A. Lecocq, M. Petit, V. Sauvant-Moynot, and F. Huet, "Safety focused modeling of lithium-ion batteries: A review," *Journal of Power Sources*, vol. 306, pp. 178 – 192, 2016.

[85] A. F. Blum and R. T. Long Jr, "Hazard assessment of lithium ion battery energy storage systems," Fire Protection Research Foundation, Tech. Rep., Feb. 2016. [Online]. Available: https://www.nfpa.org/-/media/Files/News-and-Research/Fire-statistics-and-reports/Hazardous-materials/RFFireHazardAssessmentLithiumIonBattery.ashx

[86] Kauai Island Utility Cooperative (KIUC), "Schedule Q addendum and FAQs," 2019. [Online]. Available: https://website.kiuc.coop/sites/kiuc/files/documents/Schedule Q Curtailment FAQ March 2019 FINAL ATT.pdf

[87] Hawaiian Electric (HECO), "Customer renewable energy programs billing and credit." [Online]. Available: https://www.hawaiianelectric.com/documents/products_and_services/customer_renewable_programs/programs_bill_and_credit.pdf

[88] G. Ravikumar, B. Hyder, and M. Govindarasu, "Hardware-in-the-loop CPS security architecture for DER monitoring and control applications," in *2020 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2020, pp. 1–5.

[89] S. N. G. Gourisetti, J. Hansen, W. Hofer, D. Manz, K. Kalsi, J. Fuller, S. Niddodi, H. Kley, C. Clarke, K. Kang, H. Reeve, M. Chiodo, and J. Bishopric, "A cyber secure communication architecture for multi-site hardware-in-the-loop co-simulation of DER control," in *2018 Resilience Week (RWS)*. IEEE, 2018, pp. 55–62.

[90] N. Duan, N. Yee, B. Salazar, J. Y. Joo, E. Stewart, and E. Cortez, "Cybersecurity analysis of distribution grid operation with distributed energy resources via co-simulation," in *2020 IEEE Power Energy Society General Meeting (PESGM)*. IEEE, 2020, pp. 1–5.

[91] O. T. Soyoye and K. C. Stefferud, "Cybersecurity risk assessment for California's smart inverter functions," in *2019 IEEE CyberPELS (CyberPELS)*. IEEE, 2019, pp. 1–5.